RQM CERT
Your Knowledge Provider

GHID ILUSTRAT

SECURITATEA ȘI SIGURANȚA UNITĂȚILOR SANITARE

ION IORDACHE
Dr. ROBERT LEU


GHID
ILUSTRAT
SECURITATEA ȘI SIGURANȚA UNITĂȚILOR SANITARE
ION IORDACHE
Dr. ROBERT LEU
PROIECT
GHIDURI ILUSTRATE
Download GRATUIT
www.rqmcert.com
www.ioniordache.com
MANAGEMENTUL OPERAȚIUNILOR DE SECURITATE
GHID ILUSTRAT
Ion Iordache
EVALUAREA DE IMPACT PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL
PENTRU SISTEMUL DE SUPRAVEGHERE VIDEO
GHID ILUSTRAT
Data Protection Impact Assessment (DPIA)
Ion Iordache
Mihai Dantis
GDPR
SUPRAVEGHEREA VIDEO
GHID ILUSTRAT
ACORD
PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL
GHID ILUSTRAT
Ion Iordache
CALCULAREA PREȚURILOR ȘI OFERTAREA
GHID ILUSTRAT
Ion Iordache
PLAN DE AFACERI
GHID ILUSTRAT
Ion Iordache
Consultanța de securitate
OFERTAREA
GHID
ILUSTRAT
HOME SECURITY
PRIVATE PROPERTY
SISTEME ȘI INSTALAȚII DE SEMNALIZARE ALARMARE ȘI ALERTARE ÎN CAZ DE INCENDIU
GHID ILUSTRAT
Ion Iordache
Marin Bulea
ANALIZA RISCURILOR LA SECURITATEA FIZICĂ
GHID ILUSTRAT
Ion Iordache
Adrian Marian Floacă
SISTEME DE ALARMĂ LA EFRACȚIE ȘI JAF ARMAT
GHID ILUSTRAT
Ion Iordache
Adrian Marian Floacă
SISTEME DE SUPRAVEGHERE VIDEO PENTRU UTILIZARE ÎN APLICAȚII DE SECURITATE
GHID ILUSTRAT
Ion Iordache
Adrian Marian Floacă
SISTEME ELECTRONICE DE CONTROL AL ACCESULUI
GHID ILUSTRAT
Ion Iordache
Adrian Marian Floacă
STANDARDE EUROPENE PENTRU SISTEMELE DE SECURITATE
PREVENIREA CRIMINALITĂȚII PRIN PROIECTAREA MEDIULUI ÎNCONJURĂTOR
GHID ILUSTRAT
CPTED
ION IORDACHE
INTELIGENȚA ARTIFICIALĂ ÎN SECURITATEA FIZICĂ
GHID ILUSTRAT
Ion Iordache
Alexandru Mihai Stoienescu
GHID
ILUSTRAT
MANAGEMENTUL RISCULUI
ȘI TEHNICI DE EVALUARE A RISCULUI
ION IORDACHE
GHID
ILUSTRAT
SECURITATEA ȘI SIGURANȚA UNITĂȚILOR DE ÎNVĂȚĂMÂNT
ION IORDACHE
FORMAREA PROFESIONALĂ
ALEGEREA FURNIZORULUI DE FORMARE
GHID ILUSTRAT
ION IORDACHE

CUVÂNT ÎNAINTE

Dragi cititori,

Ne bucurăm să vă prezentăm acest Ghid ilustrat, menit să ofere îndrumări practice pentru îmbunătățirea continuă a standardelor de securitate în toate tipurile de unități sanitare din România.

În ultimii ani, unitățile sanitare din țara noastră s-au confruntat cu provocări importante în ceea ce privește asigurarea unui mediu sigur atât pentru pacienți, cât și pentru personalul medical. De la furturi și acte de vandalism, până la amenințări cu violența și chiar agresiuni, incidentele raportate în mass-media au evidențiat necesitatea unor măsuri sporite de protecție.

Prin urmare, acest ghid vine în întâmpinarea nevoii acute de îndrumare pentru managerii de spitale, clinicile private și toți factorii responsabili cu implementarea unor protocoale adecvate de securitate. Ghidul oferă recomandări practice referitoare la controlul accesului, supraveghere video, pază și patrulare, precum și la cooperarea cu autoritățile în caz de incidente. De asemenea, sunt incluse sfaturi și exemple pentru instruirea personalului, precum și pentru crearea unei culturi organizaționale care promovează siguranța.

Sper ca informațiile cuprinse în acest ghid să contribuie la instituirea unui climat de încredere și siguranță în unitățile sanitare, în beneficiul tuturor celor implicați - pacienți, cadre medicale, personal administrativ și auxiliar.

Vă dorim mult succes în eforturile de a face din spitalele și clinicile noastre locuri primitoare și lipsite de riscuri!

Cu respect și speranță,
Ion Iordache
Robert Leu

Ion IORDACHE, Ec.

Economist de profesie și absolvent al unei școli militare de ofițeri, sunt specializat și certificat ca și consultant de securitate și trainer profesionist în educația adulților; am peste 30 de ani de experiență profesională în activități de securitate privată, evaluarea riscurilor, managementul operațiunilor de securitate, securitatea informațiilor și protecția datelor cu caracter personal, prevenirea criminalității prin proiectarea mediului înconjurător (CPTED) și educația profesională a adulților.

www.ioniordache.com; www.rqmcert.com ion@ioniordache.com; ion.iordache@rqmcert.ro

Robert LEU, Dr.

Ca medic specialist în ortopedie-traumatologie am o înțelegere profundă a nevoilor și provocărilor din sectorul medical în ceea ce privește securitatea și siguranța unităților sanitare. Sunt pasionat de domeniul securității și de aceea m-am specializat și certificat ca și manager de securitate, cu expertiză pe securitatea și siguranța unităților sanitare.

leurobert90@gmail.com

Acest ghid este dedicat tuturor unităților sanitare din România, și sperăm sincer, ca informațiile oferite să ajute managementul acestora să creeze medii de vindecare sigure și securizate utilizând îndrumările noastre orientate spre acțiune.

MULȚUMIRI!

Ghidul a fost realizat printr-o muncă de echipă, autorii, fiind ajutați de oameni pe care-i respectăm și le apreciem realizările profesionale. **Le mulțumim pentru implicare și pentru informațiile oferite!** Apreciem și mulțumim companiilor **RQM Certification** (coordonator de proiect și editor), **Verifies Integrity, Octalogik, Biconect și Spy Shop** care au oferit unele din informațiile prezentate.

Vă invit să-i cunoașteți pe Adrian-Marian, Marin, Constantin, Mihai, Sergiu, Adrian și Cristian.

Adrian-Marian FLEACĂ, Comisar-Șef de Poliție (Ing.)

Inginer electronist cu specializări și peste 20 de ani de experiență profesională în domeniul sistemelor de securitate private (evaluarea riscurilor la securitatea fizică, proiectarea, instalarea și întreținerea sistemelor electronice de securitate).

ady_sibiu77@yahoo.com

Marin BOBOC, Col. (r) Dr. Ing.

Consultant & trainer în domeniul apărării împotriva incendiilor la RQM Certification, doctor inginer, colonel de pompieri în rezervă cu specializări și peste 20 de ani de experiență profesională în domeniul apărării împotriva incendiilor (proiectarea, instalarea şi întreţinerea sistemelor sistemelor şi instalaţiilor de semnalizare, alarmare şi alertare în caz de incendiu și instalaţiilor de limitare şi stingere a incendiilor).

www.rqmcert.com marin.boboc@rqmcert.ro

Constantin IORDACHE, Ec.

Managing Partner la Verifies, companie de consultanță si management în domeniul securității private, în dezvoltarea si implementarea de soluții de securitate, care ajută companiile să selecteze si sa implementeze cele mai eficiente soluții și servicii de securitate.

www.verifies.ro iordachec@verifies.ro

Mihai DANTIS, MEng.

Lead auditor în domeniul securității informațiilor și DPO certificat international cu experiență dovedită de peste 20 de ani în managementul proiectelor, implementarea și auditul sistemelor de securitate informațională.

www.octalogik.com mihai.dantis@octalogik.com

Sergiu Dăngulea, Ing

De profesie inginer electronist, cu specializări în proiectarea, instalarea și întreținerea sistemelor electronice de securitate, Sergiu este CEO și fondatorul Spy Shop, liderul pieței online din România în distribuția de echipamente de securitate, supraveghere și monitorizare.

www. spy-shop.ro sergiu.dangulea@spy-shop.ro

Adrian Avram, Dr. Ing.

Cadru didactic la Universitatea Politehnică din Timișoara, catedra Electronică Aplicată, proiectant sisteme de securitate, cu peste 15 ani experienta in domeniul sistemelor de securitate (proiectare, instalare si intretinere).

adrian.avram@aasecurity.ro

Cristian Herbeiu, Ing.

De profesie inginer electronist, cu specializări și experiență de peste 20 ani în proiectarea, instalarea și întreținerea sistemelor electronice de securitate, a sistemelor şi instalaţiilor de semnalizare, alarmare şi alertare în caz de incendiu și instalaţiilor de limitare şi stingere a incendiilor, Cristian este fondatorul companiei BICONECT din Timișoara și trainer în cadrul RQM Certification.

www.biconect.ro cristian.herbeiu@biconect.ro

PRECIZĂRI IMPORTANTE!

Deși autorii au acordat toată atenția elaborării acestui Ghid, nu pot fi făcuți răspunzători pentru eventualele erori, inclusiv cele cauzate de neglijență. Autorii nu garantează și nu acceptă nicio responsabilitate legală care decurge din, sau în legătură cu acuratețea, fiabilitatea, actualitatea, corectitudinea sau caracterul complet al informațiilor conținute în acest ghid. Dacă, căutați sfaturi cu privire la cerințele dvs. specifice securității unității sanitare, autorii și coautorii (**cu excepția lui Adrian-Marian Fleacă**) pot acorda consultanță pe bază de contract. Sprijinim și încurajăm diseminarea și schimbul de informații realizând o cercetare rezonabilă pentru a identifica materialele deținute de terți utilizate în informarea din cadrul acestui ghid; referințele utilizate, și alte surse de informare sunt prezentate în Bibliografie.

CUPRINS:

INTRODUCERE

Foto: freepik.com, @upklyak

Toate unitățile sanitare, indiferent de tipul lor, spitalele și toate unitățile asimilate spitalelor, centrele de sănătate, centrele medicale, centrele de diagnostic și tratament, institutele, clinicile medicale, sanatoriile dar și unitățile mai mici cum sunt dispensarele medicale, cabinetele independente de medicină de familie sau de medicină generală, cabinetele stomatologice sau farmaciile și depozitele farmaceutice trebuie să facă față unor provocări specifice în materie de securitate și siguranță.

Toate aceste unități sanitare acordă prioritate creării unei atmosfere primitoare și accesibile, în care personalul, pacienții și vizitatorii să se poată deplasa cu un anumit grad de mobilitate în timp ce primesc îngrijiri, își vizitează apropiații și oferă îngrijiri, în unele situații, în cadrul unor facilități uriașe și complicate.

De exemplu, un pacient al unui spital ar putea fi nevoit să viziteze un medic, un centru de imagistică și, eventual, un laborator, toate în aceeași zi, ceea ce necesită deplasarea în mai multe locații răspândite în diverse clădiri ale spitalului.

Se așteaptă ca toate unitățile sanitare să mențină un mediu sigur și să se pregătească pentru o varietate de pericole potențiale, inclusiv pacienți instabili sau cu deficiențe, conflicte între pacienți, între pacienți și familiile acestora, sau chiar conflicte generate de angajați actuali sau foști, nemulțumiți.

Actele de violență, potențialul de criminalitate și chiar de terorism, precum și răspunsul la incidentele de urgență și atenuarea efectelor acestora reprezintă preocupări semnificative pentru toate unitățile sanitare.

Deși există prevederi și obligații legale clare pentru a asigura securitatea și siguranța unităților sanitare în România, în puține cazuri măsurile luate sunt suficiente și eficiente. Motivele sunt multiple, dar amintesc aici doar pe cele mai vizibile. Uneori, lipsa de interes a autorităților și/sau a managementului unităților sanitare, alteori lipsa unui personal de securitate competent sau alegerea unor furnizori de servicii de securitate ineficienți și nu în ultimul rând, bugetul insuficient.

În ultimii ani, alarmate de mai multe evenimente, unele tragice, în care s-au pierdut vieți omenești și au avut loc pagube materiale uriașe, multe unități sanitare din România au început să-și modernizeze sistemele de securitate și să caute profesioniștii adevărați pentru a asigura o securitate și o siguranță eficientă în protecția vieților oamenilor și bunurilor din interiorul/exteriorul acestora.

Anticipăm că această tendință va continua pe măsură ce unitățile sanitare, indiferent de forma de organizare, caută o mai mare securitate din cauza creșterii violenței generate de pacienți și/sau vizitatori, a provocărilor generate de lipsa de personal (medici și asistente medicale, de exemplu) a furturilor sau alte acte infracționale.

Nevoia de securitate/siguranță sporită, reprezintă o provocare fără precedent în ceea ce privește metodele de protecție a unităților sanitare, asigurarea securității și siguranței acestora depășind, uneori, departamentul de securitate intern. Pentru a atinge un nivel ridicat, sau măcar optim de securitate, autoritățile locale, managerii și consiliile de administrație trebuie să se implice mai mult, prin niveluri de finanțare adecvate, în gestionarea și susținerea securității/siguranței și a altor aspecte legate de gestionarea riscurilor de securitate ale unităților sanitare.

Orientările din acest ghid sunt menite să ofere îndrumări managerilor și consiliilor de administrație ale unităților sanitare, practicienilor din domeniul securității medicale, dar și autorităților locale, pentru a se asigura că aceste bune practici sunt luate în considerare și integrate, acolo unde este posibil, în fiecare spațiu existent, nou sau renovat.

TERMENI ȘI DEFINIȚII

securitate fizică - starea de fapt în care riscul determinat de factorii de ameninţare şi vulnerabilităţile care pot pune în pericol viaţa, integritatea corporală sau libertatea persoanei ori pot aduce prejudicii valorilor deţinute de unităţi se situează la un nivel acceptabil;

ameninţare - factor intern sau extern ce are capacitatea de a exploata vulnerabilitatea unei unităţi prin acte sau fapte ce creează dezechilibre ori instabilităţi şi generează stări de pericol asupra vieţii, integrităţii corporale sau libertăţii persoanelor ori valorilor deţinute;

vulnerabilitate - caracteristică de ordin fizic-arhitectural şi operaţional a unei entităţi, prin care aceasta este expusă distrugerii, agresiunii ori disfuncţionalităţii în faţa unei ameninţări;

analiza de risc la securitatea fizică - activitate desfăşurată pentru a identifica ameninţările şi vulnerabilităţile care pot pune în pericol viaţa, integritatea corporală sau libertatea persoanei ori care pot aduce prejudicii valorilor deţinute de unităţi, în scopul determinării impactului şi evaluării riscurilor de securitate şi în baza căreia se stabilesc măsurile necesare pentru limitarea sau eliminarea acestora;

incident de securitate - eveniment produs, având o evoluţie necontrolată, care generează consecinţe nedorite asupra persoanelor şi/sau valorilor, şi/sau activităţilor în cadrul unei unităţi şi care necesită o acţiune imediată pentru restabilirea situaţiei anterioare;

zona perimetrală - limita fizică a construcţiei, constituită din elemente fixe sau mobile, cum ar fi: pereţi, vitraje sau ferestre;

măsură de securitate - componenta de bază a unei soluţii de securitate, corespunzătoare uneia sau mai multor ameninţări şi vulnerabilităţi identificate conform analizei de risc şi care are ca scop reducerea riscurilor asociate;

mecanisme de securitate - soluţii care cuprind mai multe măsuri de securitate, care funcţionează conform unor scenarii predefinite, pentru securizarea unuia sau mai multor obiective, atunci când sunt amplasate în acelaşi perimetru;

sistem de securitate - ansamblu integrat de măsuri organizatorice, tehnice şi procedurale care are ca scop obţinerea securităţii fizice pentru o organizaţie sau un obiectiv;

zona de acces în unitate - locul amenajat cu elemente de închidere nestructurale destinate intrării sau ieşirii persoanelor; căile de acces pot fi dedicate clienţilor, angajaţilor, transferului valorilor sau mixte;

zona de tranzacţionare - spaţiul în care operatorii manipulează valorile monetare sau bunurile în relaţia cu clienţii;

zona de transfer - spaţiile prin care se vehiculează valorile între locul de depozitare şi alte zone interioare sau exterioare în cazul transportului;

zona echipamentelor de securitate - spaţiul restricţionat accesului persoanelor neautorizate, destinat amplasării, funcţionării sau monitorizării unor astfel de echipamente;

zona de depozitare - spaţiul special amenajat pentru păstrarea în siguranţă a valorilor monetare ori a bunurilor;

zona de expunere - spaţiul amenajat pentru prezentarea către public, în condiţii de siguranţă, a bunurilor sau valorilor;

sistem de management al situațiilor de pericol - sistem de afișare și gestionare a mesajelor de pericol transmise de sistemele de detectare a incendiilor și de alte sisteme conectate;

sistem de alarmă - instalaţie electrică care răspunde la detectarea manuală sau automată a prezenţei unui pericol; sistemul de alarmare la efracţie este alcătuit din: centrala de alarmă cu tastaturile de operare, elementele de detecţie, echipamentele de avertizare şi semnalizare şi alte componente specifice acestui tip de aplicaţii;

sistem de supraveghere video (sistem de televiziune cu circuit închis) - sistem compus din echipamentul camerei, echipamentul de monitorizare şi echipamentul asociat pentru transmisie şi control, care ar putea fi necesar pentru supravegherea unui zone protejate; are în componenţă camerele video, echipamentele de multiplexare, stocare şi posibilitatea de vizualizare a imaginilor preluate, în vederea observării, recunoaşterii şi/sau identificării persoanelor.

sistem de control al accesului - sistem conceput să permită persoanelor autorizate intrarea şi ieşirea dintr-o zonă de securitate controlată şi să refuze o astfel de intrare sau ieşire persoanelor neautorizate, ce cuprinde unitatea centrală, care gestionează punctele de control, unităţile de comandă, cititoarele, încuietorile sau dispozitivele electromagnetice de acţionare a uşilor, şi are rolul de restricţionare a accesului neautorizat în spaţiile protejate;

instalație de detectare, semnalizare și alarmare incendiu (IDSAI) - ansamblu complex de echipamente electrice care are rolul de a asigura supravegherea unei clădiri, sau incinte în vederea detectării, semnalizării și avertizării asupra izbucnirii unui incendiu, în timp util intervenției în sensul localizării și acționării împotriva acestuia.

CAPITOLUL 1

MEDIUL DE ASISTENȚĂ MEDICALĂ

Acest capitol descrie mediul de asistență medicală, cu nevoi specifice de protecție.

Definește securitatea ca un sistem de garanții, cu rolul de a diminua riscurile și a minimaliza daunele, neîncetând a se adapta condițiilor de mediu.

Evidențiază necesitatea unei viziuni corecte a securității, distincția dintre remedierea administrativă și aplicarea legii, și rolul acestora în rezolvarea situațiilor critice.

PROTEJAREA MEDIULUI DE
ASISTENȚĂ MEDICALĂ

Motivul principal pentru asigurarea securității și siguranței în mediul medical este datoria morală a organizației de a minimiza riscul de rănire sau deces pentru pacienți și personal.

De asemenea, există responsabilități legale și contractuale ale organizației față de pacienți. Acestea contribuie la furnizarea de îngrijiri de calitate, menținerea bazei economice a organizației și menținerea relațiilor sănătoase cu publicul, comunitatea și personalul.

Securitatea și siguranța sunt concepte înrudite, dar au semnificații diferite.

Siguranța se referă la condiția de a fi protejat de rău sau de pericol și se poate aplica atât la siguranța fizică, cum ar fi protecția împotriva accidentelor, rănilor sau dezastrelor naturale, cât și la siguranța emoțională și psihologică, cum ar fi protecția împotriva abuzurilor, hărțuirii sau intimidării.

Securitatea, pe de altă parte, se referă la măsurile luate pentru a se proteja împotriva daunelor sau amenințărilor intenționate, cum ar fi furtul, atacurile cibernetice, terorismul sau alte activități criminale și poate include măsuri de securitate fizică, cum ar fi încuietori, alarme și camere de supraveghere, precum și măsuri de securitate digitală, cum ar fi firewall-uri și criptare.

În timp ce, atât siguranța, cât și securitatea se referă la protecție și prevenire, siguranța se concentrează de obicei pe daunele neintenționate, în timp ce securitatea se referă la daunele intenționate.

Măsurile de siguranță sunt adesea orientate spre prevenirea accidentelor sau atenuarea efectelor acestora, în timp ce măsurile de securitate se concentrează pe prevenirea daunelor intenționate și pe reducerea la minimum a impactului încălcărilor de securitate.

Asigurarea unei securități și a unei siguranțe adecvate în unitățile sanitare este determinată de o varietate de motive, inclusiv de obligația morală, responsabilitatea juridică, respectarea cerințelor de acreditare și de reglementare, calitatea îngrijirii pacienților, stabilitatea economică și bunele relații publice.

Unitatea sanitară are obligația morală de a-și proteja pacienții și bunurile, precum și obligația legală de a-și gestiona în mod corespunzător operațiunile.

Asigurarea securității și siguranței contribuie, de asemenea, la asigurarea unei îngrijiri de calitate pentru pacienți, la menținerea stabilității financiare a unității sanitare și la construirea unor relații pozitive cu publicul, comunitatea și personalul.

De exemplu, menținerea siguranței și securității este crucială pentru prevenirea incendiilor. Este de așteptat ca securitatea să sprijine direct eforturile de menținere a siguranței prin raportarea riscurilor, raportarea erorilor și/sau raportarea actelor de neglijență.

Prevenirea accidentelor este principalul obiectiv al eforturilor de securitate care solicită identificarea riscurilor de securitate despre care vom discuta, pe larg,în capitolele următoare.

Pe scurt:

- **siguranța se referă la protecția împotriva vătămărilor neintenționate, în timp ce**
- **securitatea se referă la protecția împotriva vătămărilor sau amenințărilor intenționate.**

Un sistem de securitate într-o unitate sanitară este creat prin aplicarea unor măsuri de securitate pentru a gestiona vulnerabilitățile și riscurile de securitate identificate.

Aceste măsuri pot fi împărțite în două categorii: măsuri fizice (cum ar fi iluminatul) și măsuri psihologice (cum ar fi camerele de luat vederi)

Măsurile fizice oferă un element psihologic de protecție, cum ar fi faptul că servesc drept factor de descurajare. Camerele de supraveghere video, de exemplu, servesc drept factor de descurajare psihologică, deoarece infractorii pot să nu cunoască amploarea sistemului și să se întrebe dacă sunt supravegheați sau dacă imaginile captate sunt dovezi.

Măsuri comune de securitate psihologică și fizică

Psihologică	Fizică
Semnalizare/Monitoare de afișare video	Agenți de securitate
Ecusoane vizitatori/Jurnale de intrare	Alarme
Marcarea/Etichetarea	Supraveghere video
Investigarea incidentelor agresive	Ferestre
Politica de control al accesului	Bariere
Condiții de muncă	Iluminat
Măsuri disciplinare de muncă	Seifuri/containere
Recunoașterea personalului	Controale de acces
Găsirea drumului și îndrumare	Ecusoane de identificare
Proiectare peisagistică/Arhitectură	Dispozitive de comunicare în caz de urgență

Factorii psihologici de descurajare

Factorii psihologici de descurajare reprezintă o parte importantă a planificării securității, deoarece aceștia vizează procesul decizional al individului.

Prevenirea criminalității prin proiectarea mediului (CPTED) utilizează mediul fizic și alte aspecte ale proiectării pentru a gestiona comportamentul, cu scopul de a reduce incidența și teama de criminalitate, precum și de a influența comportamentul oamenilor prin furnizarea de factori de descurajare psihologici și fiziologici.

De asemenea, **factorii psihologici de descurajare sunt utilizați pentru a inhiba comportamentul negativ și pentru a crea un sentiment de securitate** dar crearea unui sentiment fals de securitate poate avea implicații juridice și implică securitatea fizică, semnalizarea sau materiale scrise care exagerează nivelul de protecție oferit.

Exemple de falsă securitate sunt camerele de supraveghere video false și panourile cu anunțuri care pretind că există o patrulă de securitate sau supraveghere electronică, când nu este cazul.

Dacă măsurile normale de securitate sunt compromise sau absente, trebuie să se implementeze o măsură de protecție suplimentară pentru a atenua riscul cauzat de absența măsurii de protecție.

Sistemul de securitate fizică și de descurajare psihologică din cadrul unităților sanitare este conceput pentru a preveni cât mai multe acte infracționale posibile.

Nivelul de securitate este o decizie de management bazată pe valoarea sau importanța pe care organizația o acordă securității și pe toleranța sa la risc.

Cu toate acestea, este important de reținut că nicio măsură de securitate nu va fi perfectă și suficientă pentru a-i descuraja pe toți potențialii infractori.

Concluzii:

Obiectivele de bază ale unui programului de securitate în unitățile sanitare ar putea avea următoarele roluri:

- să contribuie la misiunea generală a unității sanitare în ceea ce privește furnizarea de servicii de îngrijire medicală excelente;
- să prevină incidentele legate de securitate/siguranță printr-un sistem proactiv de măsuri de asigurare eficientă a securității/siguranței.
- să răspundă la incidentele de securitate astfel încât să se prevină sau cel puțin să se atenueze pagubele materiale sau vătămările corporale prin acțiuni competente și oportune;
- să creeze un sentiment de încredere în mintea personalului, pacienților și a a vizitatorilor că se află într-un mediu rezonabil de sigur și securizat.

MANAGERUL DE SECURITATE

În acest subcapitol vom face referire la funcția de securitate care ar trebui să existe în orice unitate sanitară, denumirea fiind la alegerea managementului unității dar, am considerat că utilizarea denumirii de "Manager de securitate" este mai adecvată și datorită faptului că ocupația se regăsește în COR cu codul 121306.

Funcția de securitate dintr-o unitate sanitară (managerul de securitate) trebuie privită ca un element de management care sprijină crearea mediului de asistență medicală iar acest sprijin va implica numeroase sisteme și subsisteme de servicii de protecție. Ca atare, securitatea este considerată un element al managementului unității sanitare.

O componentă obligatorie a planului de management al securității este specificarea clară a postului care are responsabilitatea pentru securitatea unității sanitare, cu un nivel de raportare clar definit pentru acest post.

Nivelul de raportare a securității în cadrul unității sanitare reflectă importanța pe care managementul o acordă funcției de securitate, precum și propria responsabilitate de a proteja persoanele și bunurile.

Unii practicieni în domeniul securității susțin că funcția de securitate trebuie să raporteze, în cazul spitalelor, de exemplu, doar managerului spitalului. Acest lucru poate suna bine în teorie, dar, în general, nu este nici practic și nici o situație satisfăcătoare.

Problema de bază este accesibilitatea.

Managerul de securitate îndeplinește funcții care, în mod necesar, nu implică în general operațiunile zilnice ale departamentului neclinic dar, pe de altă parte, funcția de securitate nu trebuie să raporteze la un nivel care să-i afecteze negativ productivitatea. Funcția de securitate, la fel ca multe alte funcții din domeniul sănătății, a fost victima "aplatizării" organizaționale; diferitele niveluri de management din unitățile sanitare, care existau cândva, au dispărut.

Ca urmare, securitatea a fost adesea împinsă mai jos în ierarhia organizațională.

Aspectul important al nivelului de raportare în materie de securitate este că acesta trebuie să ofere autoritatea organizațională necesară pentru a-și îndeplini în mod corespunzător misiunea.

Practic, securitatea ar trebui să raporteze unei persoane care are atât timp, cât și interes pentru funcția de securitate. Pe scurt, trebuie să existe un sprijin de management adecvat pentru ca un program de securitate să fie eficient.

Funcția de securitate nu poate fi statică; mai degrabă, aceasta trebuie să evolueze continuu pentru a răspunde nevoilor în schimbare ale societății și trebuie să rămână flexibilă pentru a face față schimbărilor constante în ceea ce privește riscurile și vulnerabilitățile în materie de securitate care apar într-un mediu de îngrijire a pacienților, mediu aflat în schimbare și în comunitate în ansamblul său. **Este important să existe o evaluare permanentă**.

Practicienii în domeniul securității sunt de acord asupra unui aspect: funcția de securitate trebuie să fie întotdeauna înrădăcinată într-o orientare de servicii și nu bazată exclusiv pe aplicarea legii. Funcția de aplicare a legii este concepută pentru a oferi servicii de protecție din punct de vedere extern sau al mediului și nu poate oferi măsurile de protecție internă care cuprind până la 90% din sistemul de securitate al unei unități sanitare, prevenire, educație și relații publice.

Investigațiile și aplicarea politicilor de securitate sunt roluri importante ale unui program de protecție sofisticat, dar nu ar trebui să conducă structura și misiunea organizațională a departamentului de securitate.

Din experiența autorilor și a colaboratorilor la realizarea acestui ghid, putem afirma că programele de securitate tind să fie construite și dezvoltate într-o manieră care reflectă punctele forte, punctele slabe și filosofia persoanei responsabile de acestea, mai degrabă decât nevoile organizaționale.

De exemplu, dacă persoana responsabilă are o experiență de polițist programul de protecție va fi adesea structurat în direcția unui sistem puternic de prevenire și control al accesului, furturilor, uneori fiind propuse măsuri excesive de supraveghere video care pot genera probleme legale deosebite unității sanitare, sau **dacă persoana responsabilă are o experiență de pompier**, programul de protecție va fi adesea structurat în direcția unui sistem puternic de prevenire și control al incendiilor.

Acest lucru nu înseamnă că managerul de securitate nu poate elabora planul general de securitate sau nu poate oferi o contribuție direcțională, dar recomandăm ca procesul să includă reprezentanți ai managementului unității sanitare, inclusiv din departamentul de urgență, IT, resurse umane, etc.

Cu toate acestea, în cele din urmă, top managementul unității sanitare trebuie să sprijine și să dea aprobarea funcției de securitate, desemnând responsabilitatea, oferind autoritate și alocând resursele necesare pentru a pune în aplicare programul de securitate.

NOTĂ! În unitățile sanitare mai mici, măsurile de protecție vor varia semnificativ în funcție de persoana căreia i se atribuie responsabilitatea, dar în multe situații, atribuirea responsabilităților este adesea nescrisă și vagă.

De exemplu, în cazul unui cabinet medical independent de specialitate, întreaga responsabilitate revine medicului specialist care, cu siguranță, ar trebui să gestioneze un domeniu complet în afara experienței și specializării sale profesionale. Nimeni nu poate avea cunoștințe complete în toate domeniile, iar în situația prezentată, atunci când o singură persoană trebuie să îndeplinească mai multe sarcini variate, sistemul de protecție primește adesea o prioritate mai mică.

În aceste situații recomandăm apelarea la un consultant de securitate, de preferință, independent, evitându-se în acest fel incompatibilitatea cu situațiile în care el prezintă soluțiile și tot el oferă serviciile de punere în aplicare (efectuarea de servicii de pază sau de instalare a unor sisteme electronice de securitate, de exemplu).

Pentru unitățile sanitare mari, cum ar fi spitalele, institutele, centrele de sănătate, centrele medicale și clinicile medicale asimilate spitalelor **recomandăm angajarea unui "Manager de securitate" specializat în securitatea unităților sanitare și/sau căruia să i se asigure accesul la pregătirea profesională specifică sistemului medical.**

MANAGEMENTUL ȘI PLANIFICAREA RISCURILOR DE SECURITATE

Protecția unei unități sanitare începe cu identificarea amenințărilor potențiale și cu evaluarea impactului acestora în cazul în care s-ar produce.

Amenințările pot fi fie dezastre naturale, fie incidente provocate de om și pot duce la daune materiale, întreruperea activității, pierderi, răniri sau decese.

Analiza vulnerabilității la riscuri (Hazard Vulnerability Analysis - HVA) este o componentă cheie în planificarea și gestionarea unităților sanitare.

Aceasta oferă o abordare structurală de evaluare a riscurilor potențiale pe care o unitate sanitară le-ar putea întâmpina, acoperind o gamă largă de pericole, de la incidente legate de securitate până la dezastre naturale.

Un aspect principal al HVA este identificarea și categorizarea riscurilor specifice pentru un anumit centru medical.

Aceste riscuri pot varia considerabil în funcție de o serie de factori, inclusiv locația fizică a unității, populația pe care o servește și natura specifică a serviciilor pe care le oferă.

De exemplu, un spital aflat într-o zonă urbană dens populată poate fi supus unor riscuri diferite de cele ale unei clinici dintr-o zonă rurală sau de o unitate medicală specializată în îngrijirea pacienților cu boli infecțioase.

În cadrul HVA, vulnerabilitățile de securitate sunt luate în considerare ca parte a unei abordări "all-hazards".

Asta înseamnă că unitatea medicală nu doar că se pregătește pentru evenimente de securitate obișnuite, precum furtul sau agresiunea, dar este pregătită și pentru incidente mai largi și potențial mai devastatoare, precum dezastrele naturale sau atacurile teroriste.

Abordarea "all-hazards" recunoaște faptul că orice incident, indiferent de originea sau natura sa, poate avea un impact asupra funcționării normale a unei unități de sănătate și, prin urmare, trebuie gestionat corespunzător.

Partea de atenuare a HVA se referă la măsurile proactive pe care o unitate de sănătate le poate lua pentru a limita impactul unui eveniment potențial.

Aceasta poate include, de exemplu, implementarea de sisteme de securitate mai robuste, crearea de planuri de evacuare, instruirea personalului pentru situații de urgență și investirea în rezerve de echipamente și provizii de urgență.

În sfârșit, analiza HVA presupune evaluarea fiecărui risc pe baza probabilității sale de a apărea și a consecințelor potențiale sau a daunelor care ar putea rezulta. Acest proces de evaluare îi permite unității de sănătate să prioritizeze riscurile și să aloce resursele în mod corespunzător pentru a se pregăti și a atenua aceste riscuri.

De exemplu, un spital situat într-o zonă cu frecvente cutremure ar putea acorda o prioritate mai mare pregătirii pentru un astfel de eveniment în comparație cu alte tipuri de riscuri.

Conform autorilor Tony W. York & Don MacAlister, în lucrarea "Hospital and Healthcare Security" toate unitățile sanitare, indiferent de mărime, se confruntă cu riscuri de securitate de bază, care au fost grupate în 21 de categorii majore.

Magnitudinea fiecărei categorii de risc variază de la o unitate la alta și determină nivelul de amenințare pentru organizație.

Fiecare unitate trebuie să evalueze riscurile în mod individual și să le considere ca fiind riscuri de securitate primare, recunoscând în același timp că există și riscuri de siguranță asociate cu programul de securitate.

Toate cele 21 de categorii de risc le vom explica, în capitolul următor, pe unele mai detaliat, pe altele mai sumar.

MANAGEMENTUL RISCURILOR

Managementul riscului, în special în sectorul sănătății, este un concept relativ recent în comparație cu conceptul de securitate.

Acest domeniu a câștigat importanță în ultimii ani, în principal datorită creșterii reclamațiilor de malpraxis medical și a preocupărilor crescânde legate de siguranța pacientului.

Managerii de risc din domeniul sănătății, un grup specializat de personal de suport în cadrul unităților sanitare, joacă un rol important în acest domeniu.

Obiectivul lor principal este de a preveni prejudicierea pacientului și de a minimiza pierderile financiare pentru organizațiile de sănătate.

Pentru a realiza acest lucru, managerii de risc se ocupă adesea de o varietate de sarcini, inclusiv gestionarea contractelor, implementarea tehnologiei avansate de echipamente, administrarea asigurărilor și rezolvarea problemelor care implică potențiale sau, reale răspunderi.

Având în vedere natura muncii lor, nu este surprinzător că mulți manageri de risc au experiență în drept sau în domeniul clinic.

Structura managementului riscului poate varia între organizații.

Cu toate acestea**, este absolut esențial să existe o declarație scrisă care să definească clar funcția, autoritatea și responsabilitatea programului de management al riscului pentru funcționarea sa eficientă.**

Este de asemenea important să se considere eforturile de securitate ca parte integrantă a strategiei generale de management al riscului a organizației.

Istoric, funcțiile de securitate au raportat rar la managementul riscului. Cu toate acestea, în ultimii ani, multe organizații au reușit să schimbe această relație de raportare, integrând securitatea mai strâns cu managementul riscului.

Această schimbare s-a dovedit a fi de succes, ducând la rezultate îmbunătățite și la o abordare mai cuprinzătoare a gestionării riscului în cadrul organizațiilor de sănătate.

Dacă luăm ca exemplu, un spital, după cum se arată în figură, numeroase elemente pot fi integrate într-un program coordonat.

Componentele tipice ale managementului riscului.
(Traducere și adaptare din Hospital and Healthcare Security, Sixth Edition by Tony W. York & Don MacAlister)

PRINCIPALELE RISCURI/VULNERABILITĂȚI DE SECURITATE ÎN UNITĂȚILE SANITARE

Agresiunea - lovirea sau alte violenţe

O agresiune este un atac (neprovocat) asupra persoanelor sau bunurilor, iar Codul Penal precizează la **Art 193 Lovirea sau alte violenţe** că: ***"Lovirea sau orice acte de violenţă cauzatoare de suferinţe fizice se pedepsesc cu închisoare de la 3 luni la 2 ani sau cu amendă."***

Toate unitățile sanitare se confruntă cu o problemă serioasă de agresiuni asupra pacienților, personalului și vizitatorilor, care pot varia de la simple amenințări la atacuri grave, cum ar fi violul. Pacienții sunt deosebit de vulnerabili din cauza stării lor fizice și psihice și a accesibilității. Aceștia pot fi expuși riscului de a fi agresați de alți pacienți, vizitatori sau chiar de personalul medical. Unele agresiuni în unitățile sanitare sunt comise de furnizorii de îngrijiri și pot varia de la mângâieri până la viol. Pacienții din căminele de bătrâni sunt, de asemenea, expuși riscului de a fi agresați, inclusiv de a fi bruscați și agresați sexual. Aceste incidente pot duce la procese legate de securitate împotriva unităților sanitare.

Departamentele de urgență ale spitalelor, unitățile de terapie intensivă și zonele de tratament al sănătății comportamentale sunt frecvent scena unor agresiuni asupra personalului. În cadrul spitalului, asistentele și personalul auxiliar lucrează adesea singuri noaptea în zone îndepărtate sau au nevoie să se deplaseze prin aceste zone. Agresiunile există și în afara clădirilor unităților sanitare. Curtea interioară, parcările și străzile din jurul unității sanitare pot oferi "oportunități" pentru ca agresiunile să aibă loc.

Amenințări cu bombă

Amenințările cu bombă, care implică unitățile sanitare nu sunt la fel de răspândite în România ca în alte țări dar, cu toate acestea, riscul este foarte real, ceea ce necesită o pregătire constantă în abordarea acestui domeniu problematic de securitate.

Apelurile de amenințare cu bombă sunt imprevizibile și fiecare dintre ele trebuie luat în serios iar acțiunile întreprinse ca răspuns la o amenințare cu bombă trebuie să se bazeze pe planificarea prealabilă și pe informațiile primite în cadrul apelului.

Furturile

Intrarea ilegală, cu intenția de a comite un delict sau un furt, este un fenomen comun în unitățile sanitare. Deși s-ar putea crede că farmaciile spitalicești sunt principalele ținte, implementarea măsurilor de securitate impuse prin lege a redus numărul acestor infracțiuni. Însă, există numeroase alte ținte pentru furturi într-un spital, de exemplu, printre care se numără sălile de operații, depozitele de narcotice și anestezice, spațiile unde se păstrează bani, birourile, depozitele și zonele de lucru. Birourile medicilor și cabinetele stomatologice sunt, de asemenea, ținte frecvente, cu preponderență pentru echipamentele IT și bani. De asemenea, zonele de parcare ale spitalului constituie o sursă frecventă de furturi, necesitând măsuri de securitate preventive ridicate.

Acțiuni ale grupurilor disidente

Aceste grupuri sunt formate din persoane care are păreri sau opinii deosebite față de colectivitatea, organizația etc. din care fac parte iar experiența ne arată că acestea sunt formate dintr-un amestec de "răzvrătiți" sprijiniți de alte persoane care n-au legătură directă cu aceștia dar empatizează cu cererile lor. Acest amestec creează o provocare majoră pentru responsabilii cu securitatea din cadrul unitățile sanitare.

Controlul activităților de perturbare a ordinii publice poate fi privită ca o parte a gestionării riscurilor de securitate în cadrul planificării gestionării situațiilor de urgență.

Tulburarea ordinii şi liniştii publice

Art 371 din Codul Penal definește **tulburarea ordinii şi liniştii publice** ca ***"...fapta persoanei care, în public, prin violenţe comise împotriva persoanelor sau bunurilor ori prin ameninţări sau atingeri grave aduse demnităţii persoanelor, tulbură ordinea şi liniştea publică se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă."***

Un risc de securitate continuu pentru unitățile sanitare este reprezentat de incidentele de tulburare a ordinii și liniștii publice pentru că aceste incidente pot avea loc oriunde în interiorul sau în afara unității și pot implica pacienți, vizitatori sau personal.

Deoarece tulburările ordinii şi liniştii publice pot escalada de la certuri verbale la agresiuni și daune materiale în planul de securitate trebuie să se țină seama de mărimea, locația și tipul de unitate sanitară, precum și de tipurile de pacienți din acestea. Departamentele de primiri urgențe din marile spitale urbane reprezintă o zonă obișnuită de tulburări și necesită personal de securitate 24 de ore din 24, din cauza frecvenței ridicate a incidentelor cauzate de pacienții aflați în stare de ebrietate, sub influența drogurilor, cu deficiențe mentale, cu leziuni la cap sau aflați în custodia poliției.

Trebuie specificat că tulburările din unitățile sanitare pot proveni și din alte surse decât pacienții, cum ar fi însoțitorii acestora. Aceste incidente pot proveni din așteptări lungi, lipsa de informații, tratament necorespunzător sau confruntări domestice. Spitalele, de exemplu, recunosc necesitatea unei bune comunicări cu cei care așteaptă un tratament pentru a evita comportamentele volatile. Vizitatorii în stare de ebrietate sau influențați de droguri care cer să viziteze un pacient pot fi, de asemenea, o sursă periculoasă de probleme și necesită o intervenție rapidă pentru a controla orice escaladare. Agenții de securitate trebuie să fie pregătiți să gestioneze aceste incidente și pot fi răniți în acest proces.

Abuzul de droguri şi alte substanţe interzise

Această categorie de risc pune problema abuzului de droguri din rândul angajaților din unitățile sanitare dar trebuie să specificăm că în România acest fapt este foarte rar întâlnit iar abuzul de droguri nu este specific angajaților din domeniul sănătății. Furtul de medicamente de tip anestezic există totuși, ceea ce înseamnă că trebuie acordată o atenție sporită asigurării securității acestor medicamente.

Delapidarea

Numim delapidarea ca infracțiune care constă în însușirea, folosirea sau traficarea de către un angajat, în interesul său sau al altei persoane, a unor sume de bani sau a altor bunuri aflate în gestiunea sau în administrarea sa. Codul penal la Art 295, numește **delapidarea** ca ***"însuşirea, folosirea sau traficarea de către un funcţionar public, în interesul său ori pentru altul, de bani, valori sau alte bunuri pe care le gestionează sau le administrează se pedepseşte cu închisoarea de la 2 la 7 ani şi interzicerea exercitării dreptului de a ocupa o funcţie publică".***

Mediul sanitar reprezintă un mediu cu risc ridicat pentru delapidare și în ciuda utilizării tot mai frecvente a transferului electronic de fonduri, există încă multe "oportunități" pentru comiterea acestei infracțiuni, de exemplu.

Incendii/explozii

Aici ne referim la riscul de securitate reprezentat de incendiile provocate în unitățile sanitare, care pot duce la daune materiale semnificative și la suferințe umane.

Actele sunt, uneori, comise de angajați sau foști angajați nemulțumiți și pot apărea în perioadele de conflicte de muncă.

Unitățile sanitare ar trebui să acorde o atenție deosebită zonelor cu risc ridicat, cum ar fi depozitele, vestiarele angajaților, zonele de relaxare, camerele de echipamente, zonele de depozitare a lenjeriei, docurile de încărcare și toaletele.

Lipsirea de libertate/Răpirea

Conform Art 205 - ***Lipsirea de libertate în mod ilegal, se consideră lipsire de libertate şi răpirea unei persoane aflate în imposibilitatea de a-şi exprima voinţa ori de a se apăra dacă fapta este săvârşită: de către o persoană înarmată, asupra unui minor, pune în pericol sănătatea sau viaţa victimei, pedeapsa este închisoarea cuprinsă între 3 şi 10 ani.***

Riscul răpirilor de sugari este o preocupare pentru unitățile sanitare și pentru publicul larg. Răpirile pot fi făcute fie de un străin (acestea sunt cele mai problematice), fie de un membru al familiei.

Organizațiile din domeniul sănătății din afara României s-au confruntat cu un număr relativ mare de incidente de luare de ostatici dar în România acest risc a fost neglijabil.

Crima

În România, **omorul calificat şi tentativa de omor se pedepsesc conform Codului Penal cu detenţiune pe viaţă sau închisoare de la 15 la 25 de ani şi interzicerea exercitării unor drepturi.**

Unitățile sanitare se confruntă uneori cu incidente de omucidere în care sunt implicate diverse părți interesate, atât ca victime, cât și ca autori. Motivele includ relațiile personale, furia, disputele legate de tratamentul medical, încercările de evadare, etc. Omuciderile în domeniul asistenței medicale provin adesea din acuzații de tratament medical necorespunzător, ceea ce poate duce la represalii după o perioadă semnificativă de timp.

Furtul de identitate

Furtul de identitate are loc atunci când altcineva folosește informațiile de identificare ale unei alte persoane (de exemplu, numele, codul numeric personal, numărul cărții de credit etc.) fără permisiune, pentru a comite fraude sau alte infracțiuni.

Furtul de identitate poate avea consecințe grave pentru victime, inclusiv pierderea oportunităților de angajare, împrumuturi refuzate și arestări pe nedrept. Unitățile sanitare pot fi o țintă pentru furtul de identitate datorită, uneori, a ușurinței de acces și a vulnerabilității informațiilor personale.

Cele trei etape ale furtului de identitate includ dobândirea de informații, utilizarea informațiilor și descoperirea pierderii. Cu cât durează mai mult timp până la descoperirea furtului, cu atât mai mare este pierderea și mai mici sunt șansele de reușită a urmăririi penale. Persoanele în vârstă și pacienții sunt expuse unui risc ridicat de a fi victime ale furtului de identitate.

Impostura

Un impostor este cineva care se angajează în înșelăciune folosind un nume sau o identitate falsă. Aceasta reprezintă o vulnerabilitate comună de securitate în unitățile sanitare și implică adesea persoane care pretind a fi profesioniști din domeniul sănătății cu calificări mai mari decât au, de fapt. Acest lucru a dus la cazuri de persoane care pretind că sunt medici, acordă îngrijire și interacționează cu pacienții pentru perioade lungi înainte ca identitatea lor falsă să fie dezvăluită.

Mita

Standardul SR ISO 37001:2017 Sisteme de Management Anti-Mită definește mituirea ca ***"oferirea, promiterea, darea, acceptarea sau solicitarea unui avantaj necuvenit de orice valoare (care ar putea fi financiar sau nefinanciar), direct sau indirect și independent de locație (locații), prin violarea legislației aplicabile, ca o îndemnare sau recompensare a unei persoane pentru a acționa sau a nu acționa în legatură cu performanța îndeplinirii sarcinilor acestei persoane".***

Unitățile sanitare sunt expuse unui risc ridicat de mită cu furnizorii, datorită cheltuielilor mari și a complexității tranzacțiilor financiare. Dovedirea vinovăției în cazurile de mită poate fi dificilă, amploarea acesteia fiind greu de estimat.

Acțiuni, proteste și conflicte de muncă

O acțiune de protest este o activitate desfășurată de o organizație sindicală, dar nu este neapărat de oregulă, care produce o întrerupere a activității unei organizații. Conflictele de muncă pot duce la diverse probleme de securitate, inclusiv amenințări, hărțuire, daune materiale, intimidare, sabotaj și rănire. Problemele de protecție în timpul unei greve pot include întreruperea serviciilor, distrugerea proprietății, intimidarea și agresiunea, hărțuirea, altercațiile și potențiala compromitere a informațiilor sensibile. Aceste probleme sunt similare cu cele cu care se confruntă în timpul unei tulburări civile.

Pierderea de informații

Furtul sau utilizarea abuzivă a informațiilor confidențiale, în special a dosarelor medicale, reprezintă un risc major de securitate în toate unitățile sanitare. Acest risc a crescut odată cu apariția dosarelor medicale electronice. Pierderea de informații poate avea loc prin furtul de hardware, accesul neautorizat, rețelele nesecurizate și securitatea slabă a bazelor de date. Utilizarea sistemelor de telemedicină și tele-sănătate a creat noi oportunități de compromitere a informațiilor. Alte date de proprietate, cum ar fi rapoartele de incident, specificațiile de licitații, înregistrările financiare și documentele juridice trebuie, de asemenea, protejate în mod corespunzător. Despre acestea vom discuta în capitolul de securitatea informației.

Tâlhăria

Conform Art. 233 din Codul Penal ***"furtul săvârşit prin întrebuinţarea de violenţe sau ameninţări ori prin punerea victimei în stare de inconştienţă sau neputinţă de a se apăra, precum şi furtul urmat de întrebuinţarea unor astfel de mijloace pentru păstrarea bunului furat sau pentru înlăturarea urmelor infracţiunii ori pentru ca făptuitorul să-şi asigure scăparea se pedepsesc cu închisoarea de la 2 la 7 ani şi interzicerea exercitării unor drepturi"***. Jaful armat reprezintă o problemă de securitate semnificativă pentru unitățile sanitare, farmaciile fiind de obicei ținta principală din cauza cantității mari de medicamente pe care le au în stoc. Banii lichizi reprezintă, de asemenea, o țintă frecventă, jafurile având loc la casierii, cafenele, magazine de cadouri și alte zone în care sunt manipulați sau depozitați bani lichizi. Vizitatorii unității sanitare sunt, de asemenea, vulnerabili, ceea ce duce la relații publice negative pentru organizație.

Fuga pacientului

Aici vorbim despre pacienții care sunt incapabili să se protejeze în mod adecvat și care părăsesc unitatea de asistență medicală fără știrea și acordul personalului medical. Pacientul care pleacă pur și simplu în timpul procesului de tratament fără știrea unui îngrijitor este un incident care este denumit în general fugă.

În termeni simpli, pacientul a părăsit instituția, fie prin decizie rațională, fie din cauza capacității mentale diminuate. În acest din urmă caz, pacientul este expus unor posibile vătămări corporale sau chiar morții în ceea ce privește vremea, accidentele sau faptul că nu a luat medicamente/tratamente care să-i salveze viața.

Hărțuirea

Conform Art. 208 din Codul Penal, **hărțuirea** este ***"fapta celui care, în mod repetat, urmăreşte, fără drept sau fără un interes legitim, o persoană ori îi supraveghează locuinţa, locul de muncă sau alte locuri frecventate de către aceasta, cauzându-i astfel o stare de temere, se pedepseşte cu închisoare de la 3 la 6 luni sau cu amendă"***.
Hărțuirea este o problemă serioasă în mediul sanitar, deoarece numărul mare de personal feminin și caracterul deschis al campusurilor centrelor medicale facilitează urmărirea victimelor de către hărțuitori.

Incidentele de hărțuire trebuie luate în serios, iar pentru a proteja victimele pot fi luate măsuri preventive proactive, cum ar fi obținerea unor ordine de restricție.

Acte de terorism

Conform Art. 295 din Codul Penal, se enumeră o serie de ***"infracțiuni atunci când sunt săvârșite în scopul tulburării grave a ordinii publice, prin intimidare, prin teroare sau prin crearea unei stări de panică".***

La modul general, terorismul este definit de utilizarea violenței sau a amenințării cu violența pentru a răspândi frica fiind o combinație de alte riscuri, cum ar fi incendiile, bombele, distrugerea proprietății și răpirile. Principalele măsuri de protecție împotriva acestuia sunt măsurile de securitate sporite, accesul restricționat și o mai mare conștientizare a bunelor practici de securitate. În general, unitățile sanitare sunt considerate ca având un risc scăzut în ceea ce privește atacurile teroriste, dar un act terorist în apropierea acestora poate avea ca rezultat daune colaterale semnificative.

Spitalele trebuie să ia în serios terorismul ca infrastructuri critice cu roluri importante în comunitate.

Furtul calificat

Conform Art. 229 din Codul Penal, **Furtul calificat** este ***furtul săvârşit în următoarele împrejurări: într-un mijloc de transport în comun; în timpul nopţii; de o persoană mascată, deghizată sau travestită; prin efracţie, escaladare sau prin folosirea fără drept a unei chei adevărate ori a unei chei mincinoase; prin scoaterea din funcţiune a sistemului de alarmă ori de supraveghere şi se pedepseşte cu închisoarea de la unu la 5 ani. Dacă furtul a fost săvârşit asupra unui bun care face parte din patrimoniul cultural; prin violare de domiciliu sau sediu profesional şi sau de o persoană având asupra sa o armă, pedeapsa este închisoarea de la 2 la 7 ani.***

Furtul de consumabile, echipamente și bunuri este o problemă comună pentru utitățile sanitare. Pierderile exacte sunt dificil de calculat și sunt adesea atribuite furtului, risipei sau lipsei de responsabilitate. Cu toate acestea, se crede pe scară largă că pierderile reprezintă un cost substanțial pentru unitățile sanitare. Printre cele mai des furate articole se numără medicamentele, lenjeria de pat, alimentele, echipamentele medicale, precum și piesele și materialele de întreținere. Furtul de echipamente este o problemă majoră pentru spitale, echipamentele medicale scumpe fiind furate frecvent.

Furturi provocate de angajați

Furturile provocate de angajați, o problemă endemică în multe sectoare ale economiei, pot fi deosebit de dăunătoare în domeniul sanitar, unde resursele pot fi atât de vitale. Aceste furturi sunt adesea responsabile pentru o proporție semnificativă a pierderilor suferite de instituțiile de sănătate. Adesea, angajații exploatează vulnerabilitățile sistemice și lipsa supravegherii adecvate, ce le oferă posibilitatea de a sustrage bunuri și resurse fără a fi detectați.

În contrast cu furtul extern, care se întâmplă ocazional și este deseori mai vizibil, furtul comis de angajați poate avea loc în mod constant și subtil, devenind o adevărată "gaură neagră" pentru resurse. În mod ironic, furturile interne pot fi mai greu de depistat și stopat, datorită încrederii și accesului pe care angajații îl au în cadrul organizației.

Sistemele de furt elaborate de către angajați pot fi uneori incredibil de sofisticate, implicând manipularea registrelor, falsificarea documentelor sau colaborarea cu alți angajați. Deși aceste cazuri pot părea excepționale, ele sunt într-adevăr perturbatoare și pot provoca pierderi masive.

Cu toate acestea, majoritatea furturilor angajate de către angajați sunt rezultatul unor oportunități aparent nevinovate și al lipsei de frică de consecințe. Un angajat poate decide să ia acasă produse de igienă, echipamente medicale sau alte resurse, convins că aceste furturi mici nu vor fi niciodată descoperite sau pedepsite. În timp, aceste furturi "mici" se adaugă, cauzând pierderi substanțiale.

EVALUAREA RISCURILOR DE SECURITATE ALE UNITĂȚILOR SANITARE

Identificarea riscurilor specifice pornește de obicei cu o revizuire a securității facilităților unității sanitare.

Identificarea și mărimea amenințărilor sau riscurilor de securitate, alături de impactul lor potențial asupra unității sanitare, reprezintă doar primii pași în protejarea organizației.

Obiectivul evaluării/analizei de securitate este să identifice punctele vulnerabile la securitate astfel încât să se poată dezvolta și implementa un plan de securitate cuprinzător, eficient și justificat din punct de vedere al costurilor. Analiza și evaluarea riscurilor oferă raționamentul pentru implementarea măsurilor de securitate (precauții) în funcție de protejarea resurselor critice, acceptând un grad calculat de risc.

Este înțeles că un activ nu poate fi protejat complet fără un cost, putem spune fără nicio reținere, extravagant sau fără a împiedica misiunea principală de a oferi îngrijire eficientă și de calitate pacienților.

Scopul implementării contramăsurilor pentru riscurile de securitate este de a face dificilă o încălcare a securității - pentru a întări facilitățile ca țintă. Gradul de dificultate de implementat depinde de valoarea activului și de toleranța organizației la risc. Când se începe procesul de evaluare a riscurilor de securitate, este important să se țină cont de diferențele subtile dintre evaluarea riscurilor, sondajul de securitate, revizuirea programului de securitate și auditul de securitate.

Evaluarea este realizată pentru a identifica și a evalua riscul de securitate prin nivelul de măsuri de protecție (precauții) existente pentru a gestiona un nivel așteptat de risc.

Un sondaj este o evaluare aleatorie a programului general pentru a determina completitudinea, acceptarea, punctele forte și punctele slabe ale programului.

Revizuirea este foarte similară cu sondajul; totuși, de multe ori se concentrează asupra unui anumit domeniu de securitate, cum ar fi departamentul de urgență, unitatea mamei și a copilului sau schimbarea în designul spațiului.

Auditul are un focus destul de îngust pentru a determina validitatea și aspectele operaționale ale unui element specific al programului de securitate.

Auditul este destinat pentru a determina dacă un element definit al sistemului de securitate funcționează în modul intenționat și produce rezultatul final așteptat.

În domeniul securității, ne referim cel mai adesea la acest termen în legătură cu revizuirea unei proceduri pentru a determina gradul de conformitate cu procesul procedurii și nevoia de a face modificări adecvate pentru identificarea necesității de instruire.

Rar securitatea devine implicată în tipurile financiare de audituri, cu excepția cazului în care este legată de o investigație.

Cine ar trebui să realizeze evaluarea riscului de securitate a unei unități sanitare?

Pentru a răspunde la această întrebare există mai multe abordări.

Prima abordare este de a delega această sarcină persoanei responsabile pentru programul de securitate de zi cu zi, managerului de securitate, despre care am discutat deja. Un avantaj al acestei abordări este că persoana respectivă posedă deja o cunoaștere generală a mediului, inclusiv problemele trecute, evaluarea comunității în ceea ce privește activitatea infracțională, filosofia organizațională și structura organizațională.

EVALUAREA RISCURILOR DE SECURITATE ALE UNITĂȚILOR SANITARE

Managerul de securitate are, cel mai probabil, un acces bun la șefii de departament și supervizori, toți aceștia fiind mai sinceri în discuția lor despre procedurile și problemele operaționale decât ar fi cu o persoană din afara organizației.

Principala îngrijorare legată de abordarea internă se referă, așa cum am prezentat deja, la calificările sale.

Simplul fapt de a ocupa o poziție nu califică pe cineva să realizeze o evaluare validă a riscului de securitate.

O persoană calificată care efectuează o evaluare a riscului de securitate în domeniul sănătății ar trebui să aibă un anumit nivel de educație și experiență, adesea validate de diverse acreditări profesionale.

A doua abordare cu privire la cine ar trebui să realizeze evaluarea de securitate este de a folosi un consultant extern.

Principalul avantaj al acestei abordări este că consultantul poate fi mai obiectiv.

Consultantul poate realiza în general sarcina de evaluare în mult mai puțin timp decât persoana internă și poate aduce o gamă largă de experiențe operaționale variate în procesul de evaluare.

Cu alte cuvinte, consultantul nu trebuie să găsească soluții de la zero și nu are conflicte de personalitate cu personalul facilității sau opinii preconcepute despre organizație.

Politicile interne și personalitățile personalului pot fi evitate sau cel puțin atenuate prin abordarea consultanților. **Principalul dezavantaj este costul consultantului.**

ATENȚIE!

Indiferent de cine realizează evaluarea, angajații văd adesea procesul, mai degrabă, ca pe o investigație, decât ca pe o revizuire a managementului afacerilor non-amenințătoare.

Managerul unuității sanitare trebuie să folosească fiecare cale disponibilă pentru a comunica părților interesate obiectivul procesului de revizuire.

Obiectivul este de a asista departamentele în performanța funcției lor specifice contribuind într-un mod pozitiv la misiunea și securitatea generală a organizației.

A treia metodă de abordare implică utilizarea unei persoane din cadrul organizației și a unui consultant extern.

Această metodă poate combina avantajele celorlalte două abordări.

Consultantul selectat pentru a "co-realiza" evaluarea trebuie să fie familiarizat cu procesul de furnizare a asistenței medicale, să aibă cunoștințe despre problemele de securitate care înconjoară mediul de asistență medicală și să aibă experiență de securitate obținută de la o varietate de facilități de asistență medicală.

Securitatea stratificată

Profesioniștii din securitate au o abordare stratificată, cu un concept circular concentric, asupra asigurării securității unui obiectiv iar acest ghid descrie abordări în patru straturi fizice pentru unitățile sanitare.

O abordare stratificată este esențială pentru abordarea unei game largi de amenințări, deoarece fiecare strat succesiv oferă componente specifice pentru a descuraja, detecta/amâna și răspunde la comportamentele adverse în cazul în care alte straturi sunt ocolite sau încălcate.

Fiecare strat include elemente de protecție de bază, sau componente, de securitate unele dintre acestea fiind comune, altele unice.

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid general privind evaluarea riscurilor de securitate în unitățile sanitare.

EVALUĂRI ALE RISCURILOR DE SECURITATE

Declarație

Evaluările riscurilor de securitate vor fi efectuate în mod regulat și continuu. Obiectivul evaluării riscurilor de securitate este acela de a identifica activele misiunii și operațiunilor primare ale unităților sanitare, amenințările și vulnerabilitățile acestor active și de a dezvolta strategii rezonabile de reducere a riscurilor pentru a proteja activele.

Intenție

A. Evaluarea riscurilor de securitate ar trebui să fie efectuată de un profesionist calificat care are pregătire și experiență în domeniul securității medicale.
B. Identificați bunurile din cadrul unității sanitare:
   1. Bunurile persoanelor pot include furnizorii de îngrijire directă și pacienții, împreună cu alte persoane, cum ar fi vizitatorii, familia și personalul de sprijin.
   2. Bunurile imobiliare includ nu numai clădirile, ci și bunurile tangibile utilizate pentru a oferi îngrijire pacienților (cum ar fi instalațiile de oxigen, echipamentele medicale, utilitățile și liniile de aprovizionare), active necorporale, cum ar fi reputația organizației și/sau datele cu caracter personal).
C. Inventarierea măsurilor de securitate actuale în vigoare pentru protejarea activelor critice, inclusiv a politicilor și procedurilor, a mijloacelor mecano-fizice, echipamente și sisteme de securitate electronice, precum și personalul de securitate.
D. Procesul de inventariere ar trebui să includă o examinare a tuturor documentelor de securitate disponibile, cum ar fi planurile de securitate, desfășurarea agenților de securitate, formarea și fișele posturilor acestora.
E. Inventarierea poate fi realizată utilizând:
   1. O abordare din exterior spre interior (începeți de la perimetru și mergeți spre activele critice identificate prin fiecare linie de apărare).
   2. O abordare de la interior la exterior (se începe de la fiecare activ critic și se continuă până la perimetru).
F. Amenințările ar trebui să fie identificate, evaluate și analizate din punct de vedere cantitativ și calitativ în raport cu lista de priorități a activelor identificate ale unității sanitare. Datele ar trebui să fie colectate din mai multe surse, inclusiv:
   1. Date interne provenite din incidentele de securitate, statisticile instalației și interviurile cu personalul.
   2. Statisticile poliției locale privind criminalitatea.
   3. Schimb de informații cu organizații similare.
   4. Alte surse de aplicare a legii.
   5. Publicații din industrie și diverse alte surse de știri.
G. Se ia în considerare îmbunătățirea protecției activelor organizației în lumina amenințărilor și a vulnerabilităților identificate pentru a determina îmbunătățirile de securitate necesare pentru a atenua riscurile. Poate fi necesară o analiză cost-beneficiu a opțiunilor pentru a selecta măsurile adecvate care să reducă riscul la un nivel acceptabil și să respecte standardele, orientările și cerințele aplicabile ale industriei de sănătate și ale agențiilor de reglementare.
H. Rezultatele evaluărilor formale ale riscurilor ar trebui să fie documentate pentru o revizuire continuă și transmise managementului.

ANALIZA DE RISC LA SECURITATEA FIZICĂ A UNITĂȚILOR SANITARE

Asigurarea securității unităților sanitare necesită o analiză a riscurilor la securitatea fizică și asta nu doar pentru că este o cerință legală.
Analiza riscurilor este, de fapt, un instrument de management, ale cărui standarde sunt determinate de orice decide managementul că este dispus să accepte în termeni de pierdere reală.
Analiza de evaluare a riscurilor este o abordare rațională și ordonată, precum și o soluție cuprinzătoare pentru identificarea problemelor și determinarea probabilității. Este, de asemenea, o metodă de estimare a pierderii așteptate din apariția unui eveniment advers.
Cuvântul cheie aici este „estimare", deoarece analiza riscului nu va fi niciodată o metodologie precisă.

ATENȚIE! Discutăm despre probabilități.

Cu toate acestea, răspunsul la majoritatea, dacă nu la toate întrebările referitoare la expunerile la securitate poate fi determinat printr-o analiză detaliată a evaluării riscurilor.

OBLIGAȚIE LEGALĂ

Ministerele şi celelalte organe de specialitate ale administraţiei publice centrale şi locale, regiile autonome, companiile şi societăţile naţionale, institutele naţionale de cercetare-dezvoltare, societăţile reglementate de Legea nr. 31/1990, republicată, cu modificările şi completările ulterioare, indiferent de natura capitalului social, precum şi alte organizaţii care deţin bunuri ori valori cu orice titlu, denumite în prezenta lege unităţi, sunt obligate să asigure paza acestora.

LEGEA nr. 333 din 8 iulie 2003 *(republicată) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, Art. 2*

Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate a obiectivelor, bunurilor şi valorilor prevăzute de lege, transpuse în planul de pază şi proiectul sistemului de alarmare.

Analiza de risc la securitatea fizică: activitate desfăşurată pentru a identifica ameninţările şi vulnerabilităţile care pot pune în pericol viaţa, integritatea corporală sau libertatea persoanei ori care pot aduce prejudicii valorilor deţinute de unităţi, în scopul determinării impactului şi evaluării riscurilor de securitate şi în baza căreia se stabilesc măsurile necesare pentru limitarea sau eliminarea acestora.

INSTRUCŢIUNILE nr. 9 din 2013 *privind efectuarea analizelor de risc la securitatea fizică a unităţilor ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelo].*

CAPITOLUL 2

PLANIFICAREA ȘI MANAGEMENTUL SECURITĂȚII

Acest capitol explorează esența planificării managementului securității în unitățile sanitare, încadrând două tipuri de planuri: Planul de Management al Securității (SMP), focalizat pe securitatea zilnică și adaptabil, și Planul Strategic de Securitate (SSP), orientat pe termen lung, care reflectă misiunea, viziunea și valorile unității.

Ambele planuri contribuie la gestionarea eficientă a securității, atât pe termen scurt, cât și pe termen lung.

PLANIFICAREA MANAGEMENTULUI SECURITĂȚII

Planificarea managementului securității este un aspect esențial pentru orice organizație, nu numai pentru unitățile sanitare.

Aceasta implică crearea a două tipuri fundamentale, dar distincte de planuri care sunt interconectate.

Aceste planuri sunt: Planul de Management al Securității [Security Management Plan (SMP)] și Planul Strategic de Securitate [Security Strategic Plan (SSP)].

Planul de Management al Securității (SMP) este primul dintre aceste două planuri fiind direct legat de programul de protecție zilnică al unității sanitare.

Caracteristica sa principală este că, SMP, este un plan pe termen scurt care se concentrează asupra prezentului, conceput pentru a fi dinamic, adaptându-se la circumstanțele și situațiile în continuă schimbare cu care se poate confrunta o unitate sanitară.

Foarte important de precizat: acest plan nu este static; este un document viu care evoluează în timp.

Necesită o revizuire formală, evaluare și modificare anuală pentru a se asigura că rămâne relevant și eficient fiind un instrument de bază pentru gestionarea nevoilor de securitate zilnice ale unității sanitare, abordând amenințările și vulnerabilitățile imediate și implementând măsuri pentru a le atenua.

Planul Strategic de Securitate, (SSP) cunoscut și sub numele de **"Security Master Plan"**, este concentrat pe termen lung deoarece se ocupă de scopurile, obiectivele și filosofia mai largă a programului de securitate al unității sanitare.

Acesta conturează direcția programului și se aliniază cu Planul Strategic al unității sanitare în ansamblu.

SSP poate fi comparat cu o "hartă rutieră" pentru că oferă un traseu clar, definit și eficient pe care unitatea sanitară să îl urmeze, ghidând-o către obiectivele sale pe termen lung.

Planul Strategic de Securitate este mai mult decât doar un plan pentru securitate; este o reflectare a misiunii, viziunii și valorilor unității sanitare și art trebui să încorporeze principiile programului de securitate ale acesteia.

Este un document de ghidare care ajută la modelarea direcției și creșterii viitoare a programului de securitate în contextul mai larg al organizației de sănătate.

Acesta asigură că programul de securitate se aliniază cu direcția strategică generală a organizației, susținându-i misiunea și viziunea, respectându-i valorile.

În concluzie, planificarea managementului securității este o abordare din două direcții care implică crearea unui Plan de Management al Securității (SMP) și a unui Plan Strategic de Securitate. Ambele planuri sunt esențiale pentru gestionarea eficientă a securității în cadrul unei unități sanitare, asigurând că poate răspunde la amenințările imediate, în timp ce planifică și pentru viitor.

PLANUL DE MANAGEMENT AL SECURITĂȚII

Un Plan de Management al Securității (SMP) este un instrument esențial pentru orice unitate sanitară, oferind o hartă pentru abordarea și atenuarea riscurilor de securitate.

Acest document, dezvoltat după o evaluare amănunțită a potențialelor amenințări la adresa organizației, ghidează programul general de protecție.

Structura SMP poate varia foarte mult, de la câteva pagini la documente extinse, în funcție de nevoile ounității sanitare. Cu toate acestea, indiferent de dimensiunea sa, planul ar trebui întotdeauna să se concentreze pe a fi operațional, abordând componentele majore ale programului de securitate, în loc de a include politici și proceduri detaliate. Gândiți-vă la acesta ca la un plan de afaceri simplificat, care exclude aspectele financiare.

Asociația Internațională pentru Securitate și Siguranță în Sănătate (IAHSS) oferă un ghid pentru crearea unui astfel de plan. Deși acest ghid conturează aspectele de bază, elementele suplimentare care ar putea fi incluse sunt:

1. O listă a măsurilor de securitate fizică ca elemente ale programului.
2. O prezentare generală a politicilor și procedurilor de funcționare ale departamentului, inclusiv protocoalele de pregătire și revizuire.
3. Identificarea personalului organizației și a altor persoane afectate de plan, cum ar fi pacienții, furnizorii, vizitatorii și comunitatea locală.
4. Standardele de performanță ale programului.
5. Strategii pentru măsurarea și îmbunătățirea programului.

Planul de Management al Securității se bazează pe o declarație a misiunii de securitate.

Această declarație, care servește ca scop al programului de securitate, ar trebui să se alinieze cu misiunea, viziunea și valorile de bază ale organizației. **Scopul SMP este de a oferi un mediu sigur și securizat pentru toate părțile implicate: pacienți, vizitatori, angajați, voluntari, personal medical și furnizori.**

Autoritatea pentru operarea zilnică a SMP ar trebui să fie clar atribuită în cadrul organizației. Această responsabilitate revine adesea unei poziții specifice desemnată de conducerea organizațională, cum ar fi un director sau manager de securitate, sau un director de facilități sau resurse umane, în special în organizațiile mai mici.

Importanța unei autorități de program este recunoscută universal în sistemele de sănătate, indiferent de țară sau nivelul de implicare a guvernului.

De exemplu, în Regatul Unit, Serviciul Național de Sănătate (NHS) cere ca fiecare Trust de Sănătate să numească un Director de Gestionare a Securității și un Specialist Local în Gestionarea Securității (LSMS), care supraveghează operațiunile zilnice.

În Canada, reglementările cer ca organizațiile de sănătate să aibă un responsabil desemnat pentru prevenirea și gestionarea agresiunilor împotriva personalului, în principal prin legislația de siguranță la locul de muncă.

Cu toate acestea, nu există o cerință specifică pentru conducerea generală a securității.

Adesea, în Planul de Management al Securității este inclusă o diagramă a organizației pentru a ilustra ierarhia de raportare deasupra poziției de administrator de securitate, de obicei până la nivelul directorului de operare.

Diagrama poate prezenta, de asemenea, organizarea departamentului sau programului de securitate, ajutând la oferirea unei înțelegeri mai clare a conceptului și structurii generale a programului de securitate.

În esență, un plan de gestionare a securității cuprinzător și bine structurat este un instrument critic care asigură siguranța și securitatea mediului unității sanitare și a părților sale interesate.

PLANUL DE MANAGEMENT AL SECURITĂȚII PENTRU SPITALUL "TIMIȘOARA"

(Exemplu fictiv)

1. Scopul planului

Planul nostru de management al securității vizează crearea unui mediu sigur și securizat pentru pacienți, angajați, vizitatori și furnizori, protejând în același timp proprietatea spitalului. În această privință, ne vom asigura că toate măsurile de securitate sunt conform standardelor și reglementărilor legale în vigoare.

2. Obiective

- Protejarea pacienților, personalului și vizitatorilor de orice potențială amenințare.
- Protejarea datelor și a informațiilor sensibile.
- Promovarea unei culturi a securității în cadrul întregii organizații.

3. Strategii

3.1 Identificarea și evaluarea riscurilor

Vom realiza evaluări periodice ale riscurilor de securitate pentru a identifica posibile amenințări și vulnerabilități și pentru a dezvolta planuri adecvate de prevenire și reacție.

3.2 Măsuri de securitate fizică

Vom asigura securitatea fizică a spitalului prin implementarea de controale adecvate, cum ar fi sisteme de supraveghere video, alarme și controlul accesului.

3.3 Securitatea informației

Vom proteja datele și informațiile sensibile printr-o varietate de măsuri, inclusiv criptare, controale de acces la date și politici stricte privind confidențialitatea.

3.4 Formare și conștientizare

Vom asigura formareaperiodică a angajaților cu privire la politici și proceduri de securitate, precum și promovarea unei culturi de securitate în întreaga organizație.

4. Responsabilități

Responsabilitatea pentru gestionarea zilnică a programului de securitate va fi atribuită Managerului de securitate. Acesta va avea responsabilitatea de a supraveghea toate aspectele planului de management al securității și de a se asigura că toate procedurile și politicile sunt respectate.

5. Revizuire și îmbunătățire

Planul de management al securității va fi revizuit în mod periodic pentru a se asigura că rămâne relevant și eficient. Aceasta va implica evaluarea incidentelor de securitate, analiza performanței sistemelor de securitate și identificarea oportunităților de îmbunătățire.

6. Concluzie

Prin implementarea acestui plan de management al securității, ne asigurăm că Spitalul "Timișoara" are un mediu sigur și protejat pentru toate părțile implicate. Ne angajăm să menținem cele mai înalte standarde de securitate și să lucrăm în mod constant pentru îmbunătățirea și adaptarea acestor standarde la orice noi provocări de securitate care pot apărea.

PLANUL STRATEGIC DE SECURITATE

Planul strategic de securitate este un cadru vital pentru organizațiile de sănătate, stabilind direcția și filosofia programului de protecție pe o perioadă mai lungă, de obicei 3-5 ani.

Acesta contrastează cu planul de management al securității de zi cu zi, concentrându-se pe elemente precum planificarea financiară, integrarea tehnologică și implementarea celor mai bune practici recunoscute în industrie.

Componente Cheie

- **Coordonarea și controlul securității la nivel de organizație:** Asigurarea unei înțelegeri clare a autorității și responsabilităților pe diferite niveluri de management.
- **Stabilitatea și implicarea în prevenirea infracționalității în vecinătate:** Concentrarea pe factorii externi care ar putea afecta securitatea organizației.
- **Coordonarea cu autoritățile:** Colaborarea cu agențiile de aplicare a legii și alte agenții de siguranță.
- **Interfața sistemului de justiție penală:** Înțelegerea și lucrul în cadrul cadrului legal.
- **Filosofia privind garanțiile de securitate fizică:** Determinarea tipului și extinderii protecțiilor fizice necesare.
- **Gradul de implicare a personalului propriu în programul de protecție:** Găsirea unui echilibru între securitatea centralizată și descentralizată.
- **Considerații privind configurația și proiectarea clădirilor:** Amplasarea fizică și modalitățile cum afectează măsurile de securitate.

Metodologii de Planificare

Există diverse abordări și procese în planificarea strategică, dar acestea implică adesea un proces în trei pași:

1. **Situația:** Evaluați situația actuală și înțelegeți cum s-a dezvoltat.
2. **Ținta:** Definiți obiective sau obiective, denumite ca starea ideală.
3. **Calea:** Trasați un traseu pentru a atinge obiectivele convenite.

Descentralizare vs. Centralizare

O întrebare cheie în planificare implică echilibrul dintre centralizarea și descentralizarea securității. De exemplu, în unitățile sanitare cu mai multe locații, trebuie luate decizii despre dacă securitatea oferă toate serviciile directe, sau dacă facilitățile individuale iau decizii independente despre raportarea evenimentelor, controlul cheilor, sistemele de alarmă, etc.

Responsabilități și Întrebări

Responsabilitățile pot varia între departamente. De exemplu, verificările de background, inclusiv istoricul infracțional, ar putea cădea exclusiv sub departamentul de resurse umane, în locul departamentului de securitate. Alte întrebări care necesită protocoale clare includ:

- Autoritatea de a chema poliția sau de a lua decizii despre încuietori și chei.
- Aprobarea și supravegherea alarmelor de securitate sau a camerelor video.
- Decizii privind finanțarea garanțiilor de securitate fizică și tipurile de echipamente.
- Procedurile pentru raportarea furturilor interne și decizii față de acestea.
- Proceduri pentru comportament neadecvat în zonele de tratament al pacienților.
- Ghiduri privind utilizarea uneltelor de forță purtate de personalul de securitate sau protocoalele scrise pentru desfășurarea echipamentelor defensive.

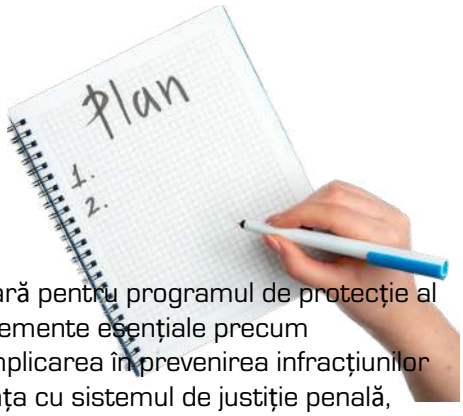
Aceste întrebări, printre altele, necesită o direcție clară și joacă un rol crucial în modelarea programului de securitate pentru unitățile sanitare.

Concluzie: Planul strategic de securitate este mai mult decât un document; este un plan de drum care integrează diverse aspecte de securitate și protecție, atât interne cât și externe, și le adaptează la nevoile și filosofia specifică a organizației de sănătate.

Necesită o planificare atentă, colaborare, reflecție și luare de decizii pentru a se asigura că sunt în vigoare măsurile de protecție potrivite, că tot personalul înțelege rolurile și responsabilitățile lor și că măsurile de securitate sunt aliniate cu cele mai bune practici ale industriei. Este o parte esențială a asigurării unui mediu sigur pentru pacienți, personal, vizitatori și proprietate în cadrul sistemului de sănătate. Abordând toate aceste fațete, planul strategic de securitate oferă o perspectivă cuprinzătoare și pe termen lung asupra protecției, permițând organizației să navigheze prin complexitățile securității moderne în sănătate cu încredere și eficacitate.

PLANUL STRATEGIC DE SECURITATE PENTRU SPITALUL "TIMIȘOARA"

(Exemplu fictiv)



1. Introducere

Acest plan strategic de securitate își propune să ofere o direcție clară pentru programul de protecție al Spitalului "Timișoara" pentru următorii cinci ani. Planul abordează elemente esențiale precum coordonarea securității la nivelul întregii organizații, stabilitatea și implicarea în prevenirea infracțiunilor în vecinătate, coordonarea cu agențiile de securitate publică, interfața cu sistemul de justiție penală, garanțiile de securitate fizică și implicarea angajaților în programul de protecție.

2. Obiective

1. Să asigurăm un mediu sigur pentru pacienți, personal, vizitatori și proprietate.
2. Să îmbunătățim și să păstrăm un nivel înalt de conștientizare a securității în rândul tuturor angajaților.
3. Să asigurăm cooperarea și coordonarea eficientă cu autoritățile de aplicare a legii.

3. Strategii

3.1 Coordonarea securității la nivel de organizație

Vom defini clar rolurile și responsabilitățile departamentului de securitate, precum și ale altor departamente, în ceea ce privește implementarea și gestionarea măsurilor de securitate. Vom promova politici de securitate centralizate pentru o gestionare eficientă a tuturor aspectelor securității.

3.2 Stabilitatea și implicarea în prevenirea criminalității în vecinătate

Vom lucra îndeaproape cu comunitatea locală și cu forțele de ordine pentru a promova un mediu sigur în vecinătatea spitalului.

3.3 Coordonarea cu agențiile de securitate publică

Vom stabili un protocol de comunicare și coordonare cu forțele de ordine locale pentru a răspunde eficient la incidente de securitate.

3.4 Interfața cu sistemul de justiție penală

Vom instrui personalul nostru în ceea ce privește legislația relevantă și vom asigura că toate procedurile de securitate respectă legile în vigoare.

3.5 Garanții de securitate fizică

Vom investi în echipamente moderne de securitate, precum sisteme de supraveghere video și control al accesului, pentru a asigura securitatea fizică a personalului, pacienților, vizitatorilor și a proprietății spitalului.

3.6 Implicarea angajaților în programul de protecție

Vom realiza sesiuni de formare regulată pentru personal pentru a îmbunătăți conștientizarea problemelor de securitate și pentru a-i ajuta să înțeleagă rolul lor în menținerea unui mediu de lucru sigur.

4. Implementare

Pentru a asigura implementarea eficientă a acestui plan strategic, vom forma o echipă de implementare a securității care să supravegheze toate aspectele procesului. Aceasta va include stabilirea de protocoale clare, monitorizarea progresului și evaluarea eficienței strategiilor implementate.

5. Evaluare

Vom evalua în mod regulat eficacitatea acestui plan strategic prin revizuirea incidentelor de securitate, prin evaluarea răspunsurilor noastre și prin ajustarea strategiilor noastre pe baza feedback-ului și a modificărilor contextului de securitate.

6. Concluzie

Acest plan strategic de securitate este conceput pentru a asigura un mediu sigur pentru toți cei care intră în contact cu Spitalul "Timișoara", aliniându-se cu cele mai bune practici ale industriei și adaptându-se continuu la noile provocări. Prin implementarea acestui plan, ne propunem să consolidăm cultura de securitate în cadrul spitalului nostru și să ne asigurăm că toate părțile interesate sunt conștiente de importanța protecției noastre colective.

PROGRAMELE DE SECURITATE ALE UNITĂȚILOR SANITARE

Programele de securitate ale unităților sanitare au un rol multifuncțional care se extinde dincolo de simpla gestionare a riscurilor și vulnerabilităților de securitate. Acestea oferă numeroase servicii, îndeplinind nevoi organizaționale esențiale.

Este important de înțeles că diferite părți ale programului de securitate în sănătate ar putea fi gestionate de diferite departamente sau indivizi.

De exemplu, verificarea antecedentelor angajaților potențiali, un element cheie al sistemului de protecție, este de obicei gestionat de departamentul de resurse umane.

Programele de securitate pentru unitățile sanitare trebuie să fie concepute având în vedere misiunea, viziunea și valorile organizaționale; designul fizic al facilității; demografia pacienților și a comunității înconjurătoare; relațiile cu angajații și publicul; resursele și bugetul disponibile; și nevoile operaționale ale facilității.

Programul trebuie să se alinieze și să susțină cultura organizației fără a împiedica obiectivul principal de a oferi îngrijire de calitate pentru pacienți.

Programele de securitate trebuie să fie dinamice, adaptându-se la schimbările societale, la schimbările mediului de îngrijire a pacienților și la evoluția riscurilor de securitate.

Acestea trebuie evaluate constant pentru a se asigura că îndeplinesc obiectivele și nevoile organizației. **Funcția de securitate (Managerul de Securitate) ar trebui să se concentreze pe orientarea către servicii, mai degrabă decât, doar pe aplicarea legii.** Deși aplicarea legii poate oferi protecție externă, salvagardările interne sunt la fel de importante și constituie până la 90% din sistemul de securitate al unei organizații, incluzând prevenția, educația și relațiile publice. Investigațiile și aplicarea politicilor sunt critice, dar nu ar trebui să determine structura și misiunea departamentului de securitate.

Designul programelor de securitate reflectă adesea punctele forte și filosofia individului care le gestionează, dar nevoile organizaționale ar trebui întotdeauna să dicteze funcția de securitate.

Managerul de Securitate poate ghida planul principal și poate oferi input, dar deciziile finale ar trebui să fie luate de echipa de management a unității sanitare, reprezentând domenii precum leadership-ul clinic, IT, resurse umane, facilități și managementul riscului.

Responsabilitățile de securitate variază semnificativ în organizațiile de sănătate mai mici și pot fi atribuite oricărui personal, de la supervizorii de asistență medicală la managerii de afaceri. Una dintre provocări este că angajații supervizează adesea domenii în afara domeniului lor de expertiză, ceea ce poate duce la o prioritate mai mică acordată sistemului de protecție.

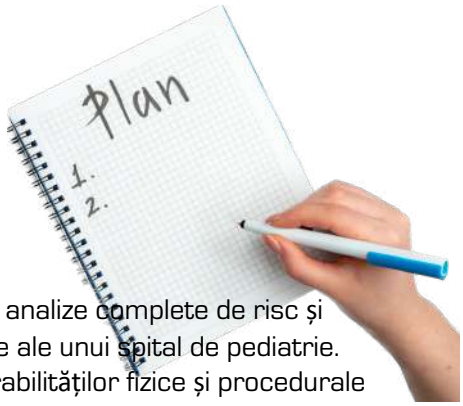
Operațiunea de securitate eficientă ar trebui să fie integrată în operațiunile de rutină ale organizației, în loc să fie impusă extern. **Pentru a maximiza rentabilitatea investiției, securitatea ar trebui să fie orientată către servicii**. Agenții de securitate joacă un rol critic în sistemul de prestare a sănătății atunci când se asimilează filosofiei de servicii. Înțelegerea modului în care rolul lor contribuie la organizație poate duce la o satisfacție mai mare în muncă, recunoaștere și potențial o plată mai mare.

Agenții de securitate oferă o varietate de servicii, de la a oferi un descurajant vizibil pentru infracțiuni la a fi disponibili pentru urgențe. Aceștia adună adesea informații de securitate valoroase prin interacțiunile cu angajații, pacienții și vizitatorii. **Un exemplu în acest sens:** o conversație a unui agent de securitate cu o receptioneră a dus la dezvăluirea unui furt într-o clinică medicală.

Rolul principal al securității în unitățile sanitare este protecția, dar acestea pot oferi, de asemenea, suport organizației în diferite moduri. Gama de funcții efectuate de un program de securitate în domeniul sănătății poate include serviciul pentru clienți, menținerea ordinii, patrularea, raportarea și investigarea incidentelor, răspunsul la solicitările de servicii, comunicarea de securitate, controlul traficului și al parcării, raportarea și investigarea accidentelor, educația și instruirea în domeniul securității, investigarea antecedentelor solicitantilor, răspunsul la urgențe interne și externe, aplicarea regulilor și reglementărilor, controlul accesului, relațiile cu aplicarea legii și agențiile guvernamentale, efectuarea auditurilor, oferirea securității fizice și electronice și oferirea a numeroase servicii de suport. **O înțelegere cuprinzătoare a acestor funcții poate ajuta la gestionarea elementelor de bază ale securității în domeniul sănătății.**

PROGRAM DE SECURITATE
PENTRU UN SPITAL DE PEDIATRIE

(Exemplu general)



1. **Analiză de risc și evaluare de securitate:** Realizarea unei analize complete de risc și evaluare a securității, concentrându-se pe nevoile specifice ale unui spital de pediatrie. Aceasta ar include analiza amenințărilor potențiale, vulnerabilităților fizice și procedurale și a impactului acestora asupra securității.

2. **Controlul accesului:** Într-un spital de pediatrie, controlul accesului este deosebit de important pentru a proteja pacienții. Sistemele de acces cu carduri și camerele de supraveghere pot fi utilizate pentru a monitoriza cine intră și iese din clădire. Un sistem de vizitatori ar putea fi de asemenea implementat, care ar putea necesita verificarea ID-urilor și a semnăturilor digitale.

3. **Securitate fizică:** Personalul de securitate ar trebui să fie prezent la punctele de intrare/ieșire și să patruleze în mod regulat coridoarele și împrejurimile spitalului. Securitatea fizică ar putea fi de asemenea îmbunătățită prin iluminarea adecvată, bariere și sisteme de alarmă.

4. **Securitate cibernetică:** Protejarea datelor pacienților este esențială. Ar trebui să fie implementate măsuri precum protecția împotriva malware-ului, criptarea datelor și backup-urile regulate.

5. **Pregătire și instruire:** Tot personalul, inclusiv angajații non-securitate, ar trebui instruit în privința politicilor și procedurilor de securitate, inclusiv cum să raporteze incidentele de securitate și cum să răspundă în cazul unui incident.

6. **Programe de prevenire a violenței:** Într-un spital de pediatrie, este posibil să se confrunte cu pacienți sau părinți supărați sau stresați. Programele de prevenire a violenței ar putea include instruirea personalului în tehnici de deescaladare a situațiilor conflictuale.

7. **Planuri de urgență și de continuitate a activității:** În cazul unui incendiu, cutremur sau alte situații de urgență, spitalul ar trebui să aibă un plan de urgență în vigoare. Acest lucru ar putea include evacuarea, comunicarea de urgență și continuitatea îngrijirii pacienților.

8. **Politici și proceduri de securitate:** Ar trebui elaborate politici și proceduri de securitate, inclusiv detaliile privind responsabilitățile personalului, procedurile de raportare a incidentelor și protocoalele de urgență.

9. **Verificarea antecedentelor angajaților:** Verificarea antecedentelor tuturor angajaților și voluntarilor este esențială pentru a asigura un mediu de lucru sigur și protejat.

10. **Relația cu forțele de ordine locale:** Etabilirea unei relații strânse cu poliția locală și cu alte agenții de aplicare a legii poate ajuta la o reacție mai rapidă și mai eficientă în caz de urgență.

Toate aceste elemente ar trebui să fie revizuite și actualizate regulat pentru a se asigura că programul de securitate rămâne eficient și relevant.

CAPITOLUL 3

PAZA ȘI PROTECȚIA

Acest capitol descrie rolul agenților de securitate în asigurarea pazei și protecției unităților sanitare.

Explică modul în care agenții asigură securitatea personalului medical, a pacienților și a bunurilor, precum și măsurile specifice pe care le iau pentru prevenirea furturilor și a altor infracțiuni.

ROLUL AGENTULUI DE SECURITATE ÎN UNITĂȚILE SANITARE

Agenții de securitate servesc ca principalul punct de contact pentru majoritatea serviciilor și activităților legate de securitate într-o unitate sanitară.

Adesea considerați a fii în prima linie a operațiunilor de securitate, acești agenți joacă un rol esențial în asigurarea securității și siguranței tuturor părților interesate. Poziția lor necesită o înțelegere cuprinzătoare a autorității lor, care formează temelia programului de securitate și a funcționării sale fără probleme.

Procesul de angajare, formare și gestionare a agenților de securitate este complex.

De la recrutarea și selecția inițială până la formarea, asigurarea diversității, determinarea compensației, motivarea și disciplinarea, fiecare pas este crucial în modelarea unei echipe de securitate competente. În contextul medical contemporan, rolul unui agent de securitate a evoluat. Ei nu mai sunt doar gardieni ai siguranței; sunt ambasadori ai serviciului pentru clienți. Obiectivul lor principal, dincolo de asigurarea securității, este de a oferi un serviciu excepțional pentru clienții unității sanitare.

Scopul final este de a promova un mediu în care profesioniștii din domeniul medical, care sunt înalt calificați și educați, pot oferi îngrijire fără nicio preocupare legată de siguranță. Echipa de securitate pune bazele acestui mediu, iar eforturile lor sunt indispensabile pentru angajați, pacienți și vizitatori.

În domeniul medical, majoritatea agenților de securitate posedă o autoritate echivalentă cu a unui cetățean obișnuit. Această autoritate, adesea definită de Poliție, autoritatea de reglementare în România în domeniul pazei și protecției, le acordă în mod tipic puterea de a interveni sau opri orice activitate infracțională pe care o observă. Rolul lor este de a reprezenta organizația pe care au sarcina să o protejeze.

Prin urmare, **autoritatea lor este o extensie a jurisdicției organizației.** Aici, jurisdicția se referă la împuternicirea legală de a exercita autoritatea. Este de o importanță primordială ca organizația să contureze clar limitele și granițele acestei autorități în politicile sale.

Cu toate acestea, **care sunt repercusiunile dacă un agent de securitate depășește sau abuzează de autoritatea sa?** Consecințele pot fi severe.

Dincolo de a se confrunta cu acțiuni disciplinare din partea organizației, agentul ar putea fi, de asemenea, supus unor acuzații penale sau procese civile.

Acuzațiile ar putea varia de la agresiune, la cele mai grave, cum ar fi omuciderea din neglijență. În plus, există numeroase acțiuni civile, cum ar fi defăimarea, detenția ilegală și calomnia, pe care o parte vătămată ar putea să le urmărească. Nu doar agentul de securitate, ca persoană este în pericol; organizația angajatoare poate fi, de asemenea, făcută responsabilă.

Chiar dacă un angajat acționează conform rolul său desemnat în fișa postului, organizația ar putea fi răspunzătoare, deoarece limitele "domeniului de angajare" pot fi uneori mai limitate decât se aștepta.

Agenții de securitate se confruntă frecvent cu situații care testează limitele autorității lor. De exemplu, dacă un pacient care așteaptă o evaluare de sănătate mintală în departamentul de urgență decide să plece înainte de a fi evaluat, poate agentul de securitate să îl rețină?

Răspunsul depinde adesea de directivele personalului clinic. Acest lucru subliniază faptul că autoritatea agentului de securitate este o extensie a mandatului organizației.

În multe locuri, absența unor legi clare privind intrarea ilegală complică lucrurile, în special atunci când se ocupă de pacienți sau vizitatori recalcitranți. În astfel de scenarii, formarea și abilitățile de comunicare ale agentului de securitate devin extrem de importante. A se baza excesiv pe intervenția poliției nu este o soluție viabilă.

PAZA PROPRIE ORGANIZATĂ DE UNITĂȚILE SANITARE

(CE SPUNE LEGEA DIN ROMÂNIA DESPRE PAZA PROPRIE ...)

LEGEA nr. 333 din 8 iulie 2003 (republicată) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor.

Articolul 1

1) Paza şi protecţia sunt activităţi desfăşurate prin forţe şi mijloace specifice, în scopul asigurării siguranţei obiectivelor, bunurilor şi valorilor împotriva oricăror acţiuni ilicite care lezează dreptul de proprietate, existenţa materială a acestora, precum şi a protejării persoanelor împotriva oricăror acte ostile care le pot periclita viaţa, integritatea fizică sau sănătatea.
2) Paza şi protecţia se realizează prin forţe şi mijloace militare sau civile, de către instituţiile specializate ale autorităţilor administraţiei publice, sau în regim privat, de către proprietarii sau deţinătorii obiectivelor, bunurilor sau valorilor, precum şi de către societăţile specializate de pază şi protecţie.

Articolul 12

1) Paza proprie se realizează cu personal calificat, angajat al unităţii beneficiare, conform legii.
2) În funcţie de numărul personalului de pază, conducerea unităţii va numi un şef de serviciu sau un împuternicit care să asigure selecţia, încadrarea, echiparea, dotarea cu armament şi mijloace de protecţie, precum şi pentru instruirea, planificarea şi controlul acestuia.
3) La unităţile unde numărul posturilor de pază este de peste 20, structura de conducere necesară este formată din şeful serviciului de pază şi şeful de tură.
4) La celelalte unităţi unde numărul de paznici este sub 20, activităţile specifice de pază se îndeplinesc de către un împuternicit al conducerii unităţii.
5) Şeful serviciului de pază sau împuternicitul cu paza se subordonează direct conducerii unităţii şi stabileşte împreună cu aceasta măsurile cele mai eficiente de pază.

Articolul 13

1) Personalul de pază proprie se compune din paznici, portari, controlori de acces sau alte persoane stabilite de conducerea unităţii, din persoanele desemnate să asigure instruirea, controlul şi coordonarea activităţii de pază. Se asimilează personalului de pază şi persoanele care cumulează atribuţiile de pază cu alte atribuţii de serviciu.
2) Personalul din paza proprie se dotează cu uniforme, echipament de protecţie şi însemne distinctive, pe care le poartă pe timpul executării serviciului.

HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003

Articolul 19

Paza proprie a obiectivelor, bunurilor sau valorilor aflate în patrimoniul unităţilor se organizează şi se execută cu personal de pază calificat şi atestat potrivit legii, aflat în raporturi de muncă sau de serviciu cu respectiva unitate.

Articolul 20

1) Angajatorul are obligaţia de a echipa personalul de pază cu uniformă, echipament de protecţie, însemne distinctive şi ecuson de identificare, precum şi de a asigura portul acestora în timpul executării serviciului.
2) Personalul de pază are obligaţia ca pe timpul executării serviciului să poarte uniforma de serviciu, echipamentul de protecţie, însemnele distinctive şi ecusonul de identificare.
3) Descrierea uniformei de serviciu, echipamentului de protecţie, însemnelor distinctive şi a ecusonului de identificare constituie anexă la planul de pază.
4) Uniforma de serviciu, echipamentul de protecţie şi însemnele distinctive se stabilesc de fiecare conducător de unitate, cu respectarea prevederilor prevăzute în anexa nr. 3.
5) Nu se pot adopta însemne, uniforme, legitimaţii, accesorii de echipament sau denumiri similare ori asemănătoare cu cele ale autorităţilor publice ale organismelor internaţionale la care România este parte.

PAZA UNITĂȚILOR SANITARE PRIN SOCIETĂȚI SPECIALIZATE

LEGEA nr. 333 din 8 iulie 2003 (republicată) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor.

Articolul 5

(1) **Paza se organizează şi se efectuează potrivit planului de pază, întocmit de unitatea ale cărei bunuri sau valori se păzesc, cu avizul de specialitate al poliţiei.** Acest aviz este obligatoriu pentru fiecare caz de modificare a planului de pază.

(4) În cazul unităţilor în care paza se asigură cu efective ale jandarmeriei, ale societăţilor specializate de pază şi protecţie, ale poliţiştilor locali sau combinat, întocmirea planului de pază se face de către conducătorii unităţilor beneficiare împreună cu comandanţii/şefii acestor efective.

Articolul 19

1) Societăţile specializate de pază şi protecţie sunt societăţi reglementate de Legea nr. 31/1990, republicată, cu modificările şi completările ulterioare, private care se constituie şi funcţionează potrivit legislaţiei comerciale şi prevederilor prezentei legi, având ca obiect de activitate paza obiectivelor, bunurilor sau valorilor, paza transporturilor de bunuri şi valori, în condiţii de maximă siguranţă a acestora, precum şi protecţia persoanelor.
2) Societăţile specializate de pază şi protecţie funcţionează în baza licenţei eliberate de Inspectoratul General al Poliţiei Române, cu avizul prealabil al Serviciului Român de Informaţii, pentru cel puţin unul dintre obiectele de activitate prevăzute la alin. (4), care poate fi reînnoită la fiecare 3 ani. Retragerea avizului prealabil al Serviciului Român de Informaţii poate constitui temei pentru anularea licenţei de funcţionare.

HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003

Articolul 1 - Paza obiectivelor, bunurilor, şi valorilor şi protecţia persoanelor prin forţe şi mijloace civile se realizează cu sprijinul şi sub coordonarea, îndrumarea şi controlul Inspectoratului General al Poliţiei Române şi al unităţilor subordonate, care urmăresc respectarea prevederilor legale în acest domeniu de activitate.

Articolul 2 – (1) În vederea îndeplinirii obligaţiilor prevăzute de Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, cu modificările şi completările ulterioare, denumită în continuare Lege, unităţile prevăzute la art. 2 alin. (1) din Lege, denumite în continuare unităţi indiferent de natura capitalului social, forma de organizare ori asociere, modul de deţinere a bunurilor ori valorilor, trebuie să adopte măsuri de securitate în formele prevăzute de Lege, completate cu măsuri procedurale.

(2) În vederea îndeplinirii obligaţiilor prevăzute de Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, cu modificările şi completările ulterioare, denumită în continuare Lege, unităţile prevăzute la art. 2 alin. (1) din Lege, denumite în continuare unităţi indiferent de natura capitalului social, forma de organizare ori asociere, modul de deţinere a bunurilor ori valorilor, trebuie să adopte măsuri de securitate în formele prevăzute de Lege, completate cu măsuri procedurale.

(3) **Cerinţele minimale de securitate, pe zone funcţionale şi categorii de unităţi, sunt prevăzute în Anexa Nr. 1.**

ATENȚIE!

Unitățile sanitare se încadrează la Articolul 8^1 din Anexa Nr.1

"Unităţile şi instituţiile de interes public trebuie să prevadă sisteme de supraveghere video pe căile de acces, holuri şi alte zone cu risc ridicat, detecţie a efracţiei pe zonele de expunere sau depozitare valori şi control acces, prin personal sau echipamente."

(4) **Adoptarea măsurilor de securitate prevăzute la alin. (1) se realizează în conformitate cu analiza de risc efectuată de unitate**, prin structuri de specialitate sau prin experţi abilitaţi, care deţin competenţe profesionale dobândite pentru ocupaţia de evaluator de risc la securitatea fizică.

EXTERNALIZAREA SERVICIILOR DE PAZĂ

Alegerea între a avea propria echipă de securitate sau a încredința serviciul unei companii externe de securitate este o decizie care depinde de diferiți factori, inclusiv bugetul, dimensiunea unității sanitare, complexitatea necesităților de securitate și disponibilitatea de a gestiona personalul de securitate intern.

Noi susținem că există multe avantaje ale contractării serviciilor de securitate, dar această afirmație nu se pot susține, întotdeauna, în practică.

Cea mai mică ofertă poate exclude calitatea, iar cele mai mari societăți de pază pretind adesea că au expertiză în domeniul securității în domeniul sănătății prin intermediul unei divizii speciale sau prin angajarea unui practician, ceea ce ar trebui examinat cu atenție.

Acestea ar putea fi cinci din avantajele și dezavantajele serviciilor contractuale de asigurare a pazei și protecției:

1. **Costurile salariale mai mici** reprezintă un avantaj principal al contractării serviciilor de securitate, dar acest lucru se realizează adesea prin plata unor salarii mici și prin utilizarea multor angajați cu fracțiune de normă. Agenții de securitate cu normă întreagă trebuie să lucreze mai mult de 40 de ore pe săptămână pentru un salariu suficient, uneori la tarife mai mici pentru ore suplimentare decât personalul intern. Orele lungi de lucru și rata mare de rotație a angajaților cu fracțiune de normă pot dăuna calității securității și continuității serviciilor. Pentru a îmbunătăți situația, acordul contractual ar trebui să includă specificații privind salariile și beneficiile pentru personalul de securitate.
2. **Contractarea serviciilor de securitate** poate scuti unitatea sanitară de sarcini administrative, dar acest lucru înseamnă și o pierdere de perspectivă și de control în atingerea obiectivelor organizației. Pentru a menține un program eficient, managementul instalațiilor trebuie să fie implicat în serviciul contractat și să acționeze ca "parteneri de afaceri" cu managementul securității contractuale. Într-un model intern sindicalizat, cerințele legate de relațiile de muncă pot consuma timpul de gestionare a securității, lăsând mai puțin timp pentru responsabilitățile de securitate corporative așteptate de unitatea sanitară.
3. **Serviciile contractuale pot furniza agenți de securitate suplimentari** în funcție de necesități, dar acest lucru poate necesita plăți suplimentare, iar personalul neinstruit poate avea o valoare limitată. În timpul unor situații de urgență, cum ar fi o inundație sau o grevă, mai mulți clienți pot avea nevoie, de asemenea, de o acoperire suplimentară, iar agențiile contractuale au limite în ceea ce privește numărul de personal pe care îl pot furniza și a cărui desfășurare poate dura mult timp.
4. **Personalul de securitate din unitățile sanitare ar trebui să aibă cunoștințe în domeniul serviciilor de securitate în domeniul sănătății**, dar societățile specializate de pază și protecție deservesc multe tipuri diferite de organizații și medii. Este dificil ca o societate specializată de pază și protecție să deservească doar spitale, de exemplu.
5. **Fraternizarea este o problemă comună în toate forțele de securitate și este prezentă și în cazul agenților de securitate contractuali.** Aceștia sunt văzuți ca persoane din afară, ceea ce poate avea atât efecte pozitive, cât și negative. Este mai puțin probabil ca agenții de securitate contractuali să dezvolte legături strânse cu personalul unității sanitare, de exemplu, ceea ce poate duce la o aplicare obiectivă a sarcinilor lor. Cu toate acestea, este posibil ca aceștia să nu aibă aceeași loialitate ca și angajații obișnuiți și să nu fie la fel de dedicați în a-și păstra locul de muncă.

CONCLUZII!

Costul unui serviciu de securitate externalizat nu ar trebui să se bazeze doar pe costul forței de muncă, ci și pe calitatea protecției oferite și pe cheltuielile anuale totale.

Angajarea unor contractori cu oferte mici poate avea ca rezultat servicii de calitate inferioară și costuri mai mari.

Managementul unității sanitare trebuie să se implice în securitatea acesteia și să nu delege responsabilitatea, exclusiv, unei terțe părți.

Un consultant în securitate poate ajuta la analiza nevoilor de securitate și poate face recomandări obiective.

OPERAȚIUNI DE SECURITATE
ÎN UNITĂȚILE SANITARE

Operațiunile de securitate în unitățile sanitare implică în principal desfășurarea personalului de securitate pentru diverse sarcini, cum ar fi patrule interioare și exterioare, monitorizarea departamentelor de urgență sau cu risc ridicat, gestionarea vizitatorilor și răspunsul la cererile de servicii de rutină și evenimente critice.

Acestea includ, de asemenea, furnizarea de servicii generale, cum ar fi direcționarea și alte funcții de servicii pentru clienți pentru a îmbunătăți experiența pacienților și a vizitatorilor.

Gestionarea eficientă a personalului, inclusiv planificarea, controlul, evaluarea și modificarea desfășurării personalului, joacă un rol crucial în succesul departamentului de securitate.

Operațiunile de securitate sunt dinamice și necesită schimbări frecvente, făcând ca desfășurarea eficientă să fie esențială**. Costul personalului de securitate necesită utilizarea sa judicioasă.** În ciuda bunelor practici din industrie și a creșterii profesionale în securitate, în general, multe programe de securitate rămân insuficient dotate, ducând la costuri excesiv de ridicate și preocupări pentru administratorii unităților sanitare.

Determinarea numărului de personal de securitate necesar implică în primul rând identificarea funcțiilor și activităților care urmează a fi realizate. Este mai precis să exprimăm nevoile de personal în termeni de echivalențe cu normă întreagă sau ore de serviciu decât prin simpla numărare a personalului.

Factori precum timpul de pregătire, concediile medicale sau concediile care fac personalul indisponibil pentru muncă ar trebui de asemenea luați în considerare.

Această calculare nu se conformează unei singure formule, ci este mai bine servită de inspectarea, răspunsul și capacitățile de prestare a serviciilor, precum și luând în considerare timpul neproductiv.

Cu toate acestea, scenariile din lumea reală exercită adesea presiuni asupra managerilor din unitățile sanitare să reacționeze rapid la incidentele de securitate prin desfășurarea mai multor persoane.

Deși un răspuns rapid este adesea necesar, decizia de a crește, sau de a reduce personalul de securitate sau aplicarea alore măsuri de protecție ar trebui să se bazeze pe o evaluare cuprinzătoare a riscurilor și vulnerabilităților de securitate actuale. Aceasta ar trebui să fie bine documentată, inclusiv raționamentul din spatele deciziilor luate.

Aplicațiile de securitate fizice și electronice, precum și politicile organizaționale afectează de asemenea numărul de personal de securitate necesar. Facilitățile cu perimetre sigure, puncte de intrare/ieșire publice desemnate și monitorizare electronică a accesului necesită de obicei mai puțin personal decât cele dintr-un mediu mai deschis. Cultura și filosofia organizației determină în mare măsură deschiderea sau restrictivitatea facilității.

Nivelul de competență și productivitatea agenților de securitate nu ar trebui omise în considerările de personal. Un agent de securitate profesionist, bine pregătit, care își execută atribuțiunile de serviciu în mod constant și la un nivel înalt poate adesea realiza mai mult decât trei agenți nepregătiți.

O strategie competitivă de compensație, asociată cu un program bine pus la punct de formare și dezvoltare pentru agenții de securitate, sunt cheia pentru a asigura un nivel ridicat de implicare și performanță constantă.

OPTIMIZAREA DESFĂȘURĂRII FORȚELOR DE SECURITATE ÎN UNITĂȚILE SANITARE

Scopul desfășurării forței de securitate în cadrul unei unități sanitare este să dispună de numărul potrivit de personal de securitate, în momentul potrivit și la locul potrivit.

Desfășurarea are patru obiective principale:

1. alocarea agenților de securitate la intervale de timp și zone cu risc mare;
2. furnizarea unui răspuns rapid la evenimentele critice;
3. acoperirea perioadelor de vârf ale fluxului de muncă;
4. asigurarea unei vizibilități înalte a forței de securitate.

Informațiile necesare pentru identificarea zonelor și momentelor cu risc ridicat se pot obține din rapoartele de incidente anterioare și din datele analizei de risc.

Hărțile generate de computer au înlocuit aproape complet hărțile tradiționale pentru reprezentarea grafică a tipurilor și locațiilor incidentelor raportate. Cu toate acestea, planurile de amplasare și documentele de configurare a clădirilor continuă să fie utile pentru prezentarea anumitor informații.

Datele statistice corespunzătoare pot fi utile pentru planificarea desfășurării și pentru ofițerii de patrulare, care pot obține rapid o imagine a problemelor dintr-o anumită zonă de patrulare.

Așteptările privind implicarea personalului de securitate în asistarea pacienților din departamentul de urgență pot avea un impact semnificativ asupra planului de personal al securității.

Se estimează că aproximativ 80% din incidentele de securitate dintr-un spital, de exemplu, provin din departamentul de urgență. O creștere a numărului de spitale cu un număr mare de pacienți cu probleme comportamentale au raportat că personalul lor de securitate interacționează cu 5-10% din pacienții lor de urgență sau persoanele care îi însoțesc pe pacienți.

Pentru aceste spitale, volumul de intervenții de securitate generate de pacienți și vizitatori este în creștere semnificativă. Cauza principală este reducerea continuă a finanțării pentru asistența în domeniul sănătății comportamentale în SUA iar aici, nici România nu este departe.

Aceasta a generat o tendință îngrijorătoare cu privire la timpul în creștere pe care agenții de securitate îl petrec cu pacienții cu risc mare în departamentul de urgență și în alte zone din cadrul unității sanitare.

Opiniile unităților sanitare variază în ceea ce privește utilizarea personalului de securitate pentru intervenții la pacienți sau supravegherea pacienților pe perioade îndelungate.

Deoarece scopul unităților sanitare este să ofere îngrijire pacienților, se poate argumenta că puține funcții de securitate ar putea fi mai importante decât sprijinirea furnizării în siguranță a îngrijirilor, prin aceste intervenții și supravegheri.

Un timp scurt de răspuns la incidentele critice este un indicator al succesului programului de securitate.

Întregul complex trebuie patrulat într-un mod care să asigure un timp de răspuns acceptabil la evenimentele critice din toate zonele unității sanitare.

Reducerea timpului de răspuns crește probabilitatea gestionării cu succes a evenimentelor nedorite. **Monitorizarea și minimizarea timpului de răspuns este poate cel mai important factor pe care o forță de securitate îl poate utiliza pentru a construi încredere și o percepție pozitivă asupra sistemului de securitate.**

Acoperirea perioadelor de vârf ale serviciilor solicitate și programate este un obiectiv important al desfășurării.

Aceste informații se obțin din experiența anterioară a unității sanitare și depind de funcțiile efectuate în programul de protecție.

Numărul de apeluri pentru serviciile de securitate este un factor important în determinarea felului în care organizația se simte cu privire la serviciul de securitate.

Un alt obiectiv al desfășurării este vizibilitatea înaltă a forței de securitate.

Această practică oferă o imagine maximă de protecție și un sentiment de securitate și siguranță pentru angajați, pacienți și vizitatori deopotrivă.

Importanța acestui factor nu poate fi supraevaluată.

OPTIMIZAREA PROCESELOR DE DOCUMENTARE ÎN PROGRAMELE DE SECURITATE

Procesul de pregătire și menținere a înregistrărilor și rapoartelor de securitate poate fi destul de intensiv în ceea ce privește resursele pentru personalul administrativ și operativ.

Cu toate acestea, un sistem de documentare eficient este o componentă esențială al oricărui program de securitate în domeniul sănătății orientat spre viitor.

Timpul și resursele dedicate documentelor și rapoartelor inutile ar putea fi folosite în schimb pentru sarcini de mai mare importanță, cum ar fi măsurile preventive împotriva incidentelor, sarcinile de investigare și furnizarea de servicii generale de securitate.

ATENȚIE! Fără colectarea, evaluarea și prezentarea corectă a datelor semnificative, devine o sarcină intimidantă pentru un program de securitate să-și demonstreze valoarea și să ia decizii bazate pe dovezi care ar putea dicta traiectoria sa viitoare în cadrul unei unități sanitare.

Provocarea cu care se confruntă managerii de securitate în sănătate contemporani, este crearea și conservarea unui sistem de documentare a programului care să satisfacă nevoile organizației. Scopul principal al unui astfel de sistem ar trebui să fie generarea și menținerea doar a acelor înregistrări și rapoarte care sunt cu adevărat necesare, în timp ce se îmbunătățește eficiența și calitatea generală a sistemului.

Este recunoscut pe scară largă faptul că un ingredient cheie al unui program de securitate eficient este un sistem de documentare complet și practic.

Colectarea bună a datelor pentru managementul performanței este critică iar menținerea documentației cu utilitate mică sau deloc poate epuiza resursele valoroase ale departamentului.

Un raport din Marea Britanie din 2014 a sugerat că organizațiile de sănătate ar putea avea nevoie să-și revizuiască prioritățile pentru personal în funcție de constatările legate de îngrijirea persoanelor în vârstă în instituțiile de îngrijire pe termen lung.

Raportul arată că interacțiunea de calitate dintre personal și pacienți poate fi compromisă deoarece personalul este preocupat de documentele obligatorii.

În contextul acestei prezentări, documentația cuprinde documente bugetare și fiscale, înregistrări de personal, politici, proceduri, corespondență, statute, contracte, rapoarte și o varietate de înregistrări specifice.

Accentul va fi pe discutarea înregistrărilor și rapoartelor operaționale folosite într-un program de securitate într-o unitate sanitară și modul în care măsurile de performanță pot fi proiectate și folosite eficient de programul de securitate pentru a ilustra calitatea, eficiența și valoarea, în concordanță cu misiunea organizațională de a oferi îngrijire de calitate pacienților.

Scopul înregistrărilor variază de la o organizație la alta, dar motivele fundamentale pentru a le menține sunt în mare parte universale.

Înregistrările oferă un sistem de memorie, facilitează schimbul de informații, ghidează procedurile operaționale, îndeplinesc diverse nevoi administrative și asistă în confirmarea activității de securitate și procesele de planificare generală.

În cadrul acestor motive primare sunt numeroase subcategorii concepute pentru a consolida eficiența și eficacitatea operațională pentru sistemul de protecție a sănătății.

Necesitatea unui sistem de memorare a acestor informații este susținută de faptul că informațiile conținute într-un raport ar putea fi necesare în câteva ore, zile sau chiar ani după finalizarea sa.

Evaluarea unui sistem de securitate implică adesea determinarea a cât mai multor întrebări despre incidente sau activități trecute sunt răspunse prin amintire personală, versus cât de multe sunt răspunse prin fapte documentate.

Operațiunile de securitate se confruntă cu provocarea inerentă de a prezice ce informații din înregistrări și rapoarte vor fi necesare în viitor.

Nu numai incidentele semnificative, dar și evenimentele minore pentru care informațiile pot fi necesare mai târziu pentru diverse motive

Procesele civile și un sistem de justiție penală supraîncărcat evidențiază necesitatea de a păstra faptele. Procesele sunt uneori intentate în ultimul moment, în speranța că informațiile de apărare de susținere vor fi pierdute, uitate sau interpretate greșit din cauza trecerii timpului.

ROLUL PERSONALULUI DE SECURITATE ÎN RELAȚIILE CU PACIENȚII

Este esențială o înțelegere clară a modului în care programul de securitate interacționează cu pacienții și vizitatorii lor în cadrul mediului de îngrijire a sănătății, pentru a îndeplini corespunzător misiunea de securitate și organizare a siguranței acestora.

Relația sau gradul de implicare a securității cu pacienții și vizitatorii unității sanitare variază în funcție de tipul de pacient, locul interacțiunii și filozofia organizației cu privire la utilizarea personalului de securitate cu pacienți cu risc ridicat.

De exemplu, agentul de securitate poate avea o responsabilitate mai mare pentru interacțiunea cu pacienții din camera de urgență din cauza prezenței fizice și necesității de a controla acest mediu, dar poate avea contact limitat cu pacienții din unitatea de sănătate mintală. **În același mod, agenții de securitate pot avea o responsabilitate mai mare în modul de interacționare cu pacienții și vizitatorii în parcările și coridoarele publice decât în camerele pacienților.**

Pacienții și vizitatorii pot fi împărțiți în două grupe distincte. Pacientul poate fi, fie un pacient ambulatoriu, fie un pacient internat. Majoritatea discuției noastre despre securitatea în domeniul sănătății se concentrează pe acest din urmă grup. În ceea ce privește vizitatorii, unii oameni vizitează un pacient internat, în timp ce alții însoțesc o persoană care caută sau primește tratament medical pe termen scurt, cum ar fi într-o cameră de urgență sau clinică.

Tipurile de vizitatori pot fi foarte diverse și includ persoane care vizitează angajații, persoane care vizitează un departament în scopuri educaționale, informaționale sau de afaceri (vânzători, furnizori, livratori, persoane care folosesc cafeneaua, etc.), și persoane care nu au un motiv legitim de a fi pe proprietate.

În România există o legislație specifică pentru drepturile și obligațiile pacienților dar, cu toate că aceasta se referă la serviciile de îngrijire directă a pacienților, toți membrii personalului de securitate ar trebui să fie conștient de aceste drepturi în ceea ce privește prestarea serviciilor de securitate. Drepturile pacienților sunt enumerate de fiecare unitate sanitară iar câteva principii de bază despre modul în care securitatea ar trebui să se angajeze și să interacționeze cu pacienții sunt notate în figură.

PERSONALUL DE SECURITATE TREBUIE SĂ-ȘI AMINTEASCĂ CĂ PACIENTUL:

- Este cel mai important element în activitatea de asistență medicală.
- Nu reprezintă o întrerupere a activității agentului de securitate, ci motivul pentru care aceasta este necesară.
- Face o favoare chemând paza; paza nu face o favoare servind pacientul.
- Face parte din afacerea de asistență medicală și nu este un străin.
- Nu este o statistică rece, ci o ființă umană cu sentimente și emoții.
- Nu este o persoană cu care să te certi sau cu care să te contrazici.
- Este o persoană cu dorințe; sarcina agentului de securitate este de a satisface unele din aceste dorințe.
- Merită cel mai politicos și atent tratament posibil.
- Face posibil ca agentul de securitate să fie plătit.

Principii de securitate de bază pentru implicarea în îngrijirea pacienților.
[Traducere și adaptare din Hospital and Healthcare Security, Sixth Edition by Tony W. York & Don MacAlister]

ROLUL PERSONALULUI DE SECURITATE ÎN RELAȚIILE CU PACIENȚII

Protecția de bază pentru pacienții interni provine de la personalul unității de îngrijiri, care constă în medici, asistente, personal de îngrijire și personal de suport auxiliar.

Este rar ca personalul de securitate să interacționeze în mod proactiv sau rutinier cu pacienții interni, deși acest lucru se întâmplă uneori în unitățile de sănătate mintală/comportamentală.

Asistența atribuită unui pacient este responsabilă pentru îngrijirea totală a acestuia, care include și siguranța pacientului.

Cu toate acestea, personalul medical primește suport din partea sistemului de securitate pentru problemele de protecție legate de pacient, la fel cum primesc suport de la alte discipline în administrarea îngrijirii medicale.

Personalul de îngrijire trebuie să fie foarte conștient de cine intră în unitate și pentru ce scop, mai ales în perioadele după program.

Așa cum rolul securității devine mai custodial în timpul orelor de noapte, îngrijirea asumă un rol mai custodial pentru siguranța pacientului.

Desigur, personalul de îngrijire are responsabilitatea în perioadele operaționale de a verifica străinii din unitate sau în camerele pacienților, dar această responsabilitate crește pe măsură ce străinii se apropie de zonele de îngrijire a pacienților în timpul nopții.

Personalul de îngrijire trebuie să fie confortabil în a relaționa cu străinii și, dacă nu este așa, să cheme securitatea.

În cele din urmă, este esențială o comunicare eficientă între personalul de îngrijire și agenții de securitate, deoarece fiecare grup percepe situațiile diferit.

Agenții de securitate trebuie să știe cum să comunice eficient cu personalul de îngrijire pentru a înțelege ce se întâmplă cu un pacient, iar personalul de îngrijire trebuie să înțeleagă necesitățile și responsabilitățile acestora pentru a integra protecția în îngrijirea pacientului.

În afara personalului de îngrijire, există multe alte persoane care vizitează în mod regulat o unitate de pacienți.

Aceștia includ voluntari, medici, terapeuți, tehnicieni și personal administrativ și de suport.

Toate aceste persoane ajută la protecția pacientului prin observarea și raportarea oricărei activități suspecte sau neobișnuite.

Mai mult, orice angajat care intră într-o cameră a pacientului are responsabilitatea de a observa și de a raporta orice semne de pericol sau risc pentru pacient.

O responsabilitate a agentului de securitate în cadrul zonei de îngrijire a pacientului este aceea de a asista personalul medical atunci când pacientul este necontrolat sau irațional.

Desigur, unele programe de securitate descurajează sau chiar interzic acest lucru.

Cu toate acestea, considerăm că acest lucru este o funcție esențială a securității care susține misiunea unității sanitare.

Acesta este un exemplu de modalitate prin care securitatea ajută la furnizarea de îngrijire medicală și poate fi un serviciu valoros pentru personalul de îngrijire și pentru pacienți.

În plus, chiar dacă acest tip de apel de asistență ar putea fi destul de rar în unele unități sanitare, în altele poate fi o rutină frecventă.

Acest lucru depinde de tipurile de pacienți pe care organizația îi servește, de disponibilitatea furnizorilor de îngrijire și de abordarea organizației față de securitate.

INVESTIGAȚIILE ÎN UNITĂȚILE SANITARE

Activitățile de investigație în cadrul programelor de securitate din domeniul sănătății joacă un rol critic și multifuncțional.

Iată un rezumat al detaliilor esențiale:

1. Funcția de investigare:

Investigațiile în unitățile sanitare nu sunt limitate la aspectele infracționale, cum ar fi furtul de medicamente sau agresiunile fizice. Deși acestea sunt aspecte esențiale, funcțiile de afaceri sunt, de asemenea, un domeniu important de investigare, care include verificări ale regulilor și regulamentelor organizaționale, încălcări ale codului de conduită, condiții de muncă nesigure și revendicări legate de hărțuire sau discriminare.

Să luăm, de exemplu, cazul unui spital care primește o serie de plângeri legate de comportamentul nepotrivit al unui angajat. Acest comportament nu este, neapărat, ilegal, dar contravine normelor de comportament stabilite de organizație, ceea ce poate afecta mediul de lucru și poate avea consecințe negative asupra pacienților.

În acest caz, departamentul de securitate sau resurse umane ar putea iniția o investigație pentru a determina validitatea acestor reclamații.

înregistrărilor video de securitate, examInvestigația ar putea include interviuri cu colegii de muncă, revizuirea inarea documentelor legate de performanța angajatului și verificarea oricăror alte informații relevante. Scopul nu este de a pedepsi infracțiuni penale, ci de a adresa problemele interne și de a îmbunătăți mediul de lucru pentru toți angajații.

Pe de altă parte, dacă există suspiciuni de fraudă financiară - de exemplu, dacă se constată că fondurile unității sanitare sunt deturnate sau facturile sunt umflate în mod artificial - atunci investigația ar căuta să identifice și să abordeze aceste probleme de afaceri.

Aceste tipuri de investigații asigură integritatea și eficacitatea operațiunilor unității sanitare și contribuie la un mediu de lucru sigur și respectuos pentru toți angajații.

Prin urmare, ele sunt o componentă vitală a programelor de securitate din domeniul sănătății.

2. Diferența față de investigațiile aplicării legii:

Investigațiile aplicării legii se concentrează în principal pe prinderea și reținerea infractorilor și colectarea de probe pentru urmărire penală. Pe de altă parte, investigațiile de securitate din domeniul sănătății sunt mai versatile, adesea conducând la remedii administrative mai degrabă decât la proceduri penale. **Rolul investigatorului este de a colecta fapte, permițând administratorilor să decidă cursul acțiunii, fie că este vorba de urmărire penală sau alte rezoluții**.

3. Stilul de Investigare:

Stilul de investigare depinde de filosofia organizației, scopul, riscurile și trăsăturile investigatorului.

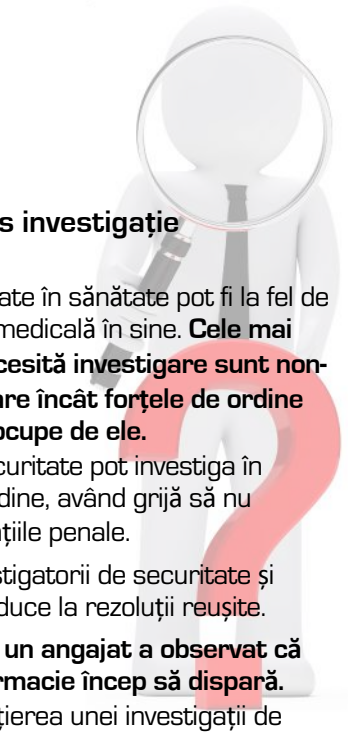
De obicei, investigațiile sunt gestionate intern, dar agențiile externe ar putea fi angajate pentru pierderi semnificative sau suspiciuni de inconduite la nivel înalt, supravegheate de consiliul juridic.

Să luăm un exemplu ipotetic: Spitalul A. Viziunea Spitalului A este una de transparență și responsabilitate, iar acest lucru se reflectă în modul în care efectuează investigațiile.

Atunci când se confruntă cu o posibilă încălcare a regulilor interne, cum ar fi hărțuirea sau discriminarea, Spitalul A își mobilizează echipa internă de securitate pentru a efectua o investigație.

Acest lucru implică interviuri cu personalul relevant, revizuirea înregistrărilor video sau documentelor și orice alte măsuri necesare pentru a aduna faptele.

În acest caz, trăsăturile investigatorului - cum ar fi atenția la detalii, abilitățile de interviu și capacitatea de a analiza datele - sunt esențiale pentru a asigura o investigație reușită.



3. Stilul de investigare:

Să presupunem că Spitalul A, descoperă dovezi ale unei posibile fraude la nivel înalt, implicând un membru al consiliului de administrație.

Acesta este un caz cu riscuri semnificative pentru organizație, atât din punct de vedere financiar, cât și din punct de vedere al reputației.

Datorită naturii delicate și complexe a acestui caz, Spitalul A decide să angajeze o agenție de investigații externe, specializată în fraude corporative.

Acest lucru nu numai că asigură un nivel mai înalt de expertiză și resurse în investigație, dar și menține obiectivitatea, evitând conflictul de interese care ar putea apărea dacă investigația ar fi condusă intern.

Totuși, pentru a se asigura că investigația este efectuată în mod corespunzător și în conformitate cu legile relevante, departamentul juridic al Spitalului A supraveghează procesul.

Avocații se consultă cu investigatorii, revizuiesc descoperirile și consiliază conducerea spitalului pe măsură ce se dezvoltă cazul.

Acest exemplu arată cum stilul de investigare poate varia în funcție de viziunea/filosofia organizației, scopul investigației, riscul pentru organizație și trăsăturile investigatorului.

4. Investigații de către diverse departamente:

Diverse departamente, precum Managementul Riscului, pot efectua investigații în domenii precum plângerile privind îngrijirea pacienților, cererile de asigurare și conformitatea cu organismele de reglementare.

Să luăm un exemplu. Spitalul B a primit plângeri repetate privind îngrijirea inadecvată a pacienților într-un anumit departament.

Departamentul de Management al Riscului, preocupat de posibilele repercusiuni juridice și de reputație, a inițiat o investigație.

Acesta a examinat documentația medicală, a intervievat personalul și pacienții, și a verificat conformitatea cu normele organismelor de reglementare.

Rezultatele au dezvăluit deficiențe în procedurile de îngrijire, iar recomandările din investigație au condus la schimbări semnificative pentru a îmbunătăți serviciile pentru pacienți și pentru a respecta reglementările.

5. Securitate versus investigație polițienească:

Investigațiile de securitate în sănătate pot fi la fel de complexe ca îngrijirea medicală în sine. **Cele mai multe condiții care necesită investigare sunt non-criminale sau minoritare încât forțele de ordine ar putea să nu se preocupe de ele.**

Departamentele de securitate pot investiga în paralel cu forțele de ordine, având grijă să nu interfereze cu investigațiile penale.

Colaborarea între investigatorii de securitate și ofițerii de poliție poate duce la rezoluții reușite.

Exemplu: în Spitalul C, un angajat a observat că medicamentele din farmacie încep să dispară.

Acest lucru a dus la inițierea unei investigații de securitate internă pentru a identifica posibilul furt.

Departamentul de securitate a început să examineze înregistrările video, să verifice înregistrările de inventar și să intervieveze personalul farmaciei.

În același timp, deoarece furtul de medicamente poate constitui un delict, poliția a fost informată și a demarat o investigație paralelă.

Securitatea spitalului și poliția au avut obiective diferite: departamentul de securitate urmărea să protejeze spitalul și să împiedice furturile viitoare, în timp ce poliția urmărea adunarea de probe suficiente pentru a inculpa și a urmări în instanță făptașul.

Pentru a evita orice interferență cu investigația poliției, managerul de securitate al spitalului a menținut contactul cu ofițerul de poliție însărcinat cu cazul.

Împreună, au colaborat și au partajat informații, rezultând în identificarea angajatului responsabil de furt și implementarea unor măsuri de securitate sporite pentru a preveni incidente viitoare.

Acest exemplu ilustrează cum securitatea și investigațiile polițienești pot funcționa în paralel pentru a aborda o problemă complexă.

6. Tipuri de investigații:

Investigațiile de securitate în domeniul sănătății pot fi împărțite în investigații operaționale (de exemplu, vandalism, furt) și investigații de nivel superior mai sensibile (de exemplu, delapidare, fraudă).

Investigatorii externi pot fi folosiți pentru obiectivitate și expertiză, adesea planificând astfel de nevoi în avans ca parte a planificării strategice.

INVESTIGAȚIA UNUI FURT DE BUNURI PERSONALE ÎN SPITALUL "TIMIȘOARA"

(Exemplu fictiv)

Prezentare proces de investigație

În cazul în care un spital este confruntat cu un furt de bunuri personale, managerul de securitate trebuie să inițieze imediat o investigație pentru a identifica autorul și pentru a preveni eventuale incidente similare în viitor.

1. **În prima etapă a investigației**, managerul de securitate ar trebui să stabilească o echipă de investigație, care să includă un reprezentant al departamentului de resurse umane și un investigator specializat în securitatea fizică a clădirilor. Echipa ar trebui să analizeze imaginile de la camerele de supraveghere, să audieze martorii și să colecteze toate informațiile relevante referitoare la momentul și locul furtului, precum și la valorile furate și la alte detalii care pot ajuta la identificarea infractorului.
2. **În urma analizei datelor colectate**, echipa de investigație ar trebui să dezvolte un profil al infractorului și să identifice posibilele motive ale acestuia. De asemenea, ar trebui să se determine modul în care infractorul a reușit să pătrundă în incintă și să ia bunurile personale, precum și să se identifice eventualele probleme de securitate ale clădirii care ar putea fi îmbunătățite pentru a preveni incidente similare în viitor.
3. **Managerul de securitate ar trebui să se asigure** că echipa de investigație lucrează în strânsă colaborare cu autoritățile competente, precum poliția și serviciul de securitate al spitalului, pentru a se asigura că toate informațiile relevante sunt analizate și că se respectă procedurile legale.
4. **În final**, managerul de securitate ar trebui să prezinte un raport detaliat al investigației, care să includă toate informațiile relevante, precum și recomandările privind măsurile de îmbunătățire a securității pentru a preveni incidente similare în viitor. De asemenea, raportarea transparentă a rezultatelor investigației poate consolida încrederea pacienților și a personalului spitalului în capacitatea de protecție a instituției.

Raport de investigație a furtului unui ceas

Data: 8 martie 2023

Obiectiv: Identificarea făptașului și recuperarea ceasului furat

Istoric: La data de 6 martie 2023, medicul pediatru dr. Andrei Popescu a raportat că a fost furat un ceas de mână de marca Rolex, în timp ce se afla la serviciu în spitalul nostru. Dr. Popescu a declarat că a lăsat ceasul în dulapul său de la birou și a constatat că acesta lipsea atunci când s-a întors după pauza de masă.

Investigația:

Am început investigația imediat după primirea raportului de la dr. Popescu. Am intervievat toți colegii de la biroul medicului, inclusiv asistentele și personalul de curățenie care au avut acces la birou în timpul pauzei de masă a medicului. În plus, am analizat înregistrările camerelor de supraveghere ale zonei în care se afla biroul medicului.

Din interviuri și analiza înregistrărilor video, am constatat că un bărbat neidentificat, în vârstă de aproximativ 35 de ani, a intrat în biroul medicului în timpul pauzei de masă a acestuia. Bărbatul a pătruns în biroul medicului, a căutat în mod intenționat prin dulapul de la birou și a furat ceasul de mână. A părăsit apoi biroul înainte de a fi văzut de cineva.

Am examinat în continuare înregistrările camerelor de supraveghere ale intrării în spital și am observat că bărbatul neidentificat a intrat în spital în dimineața zilei de 6 martie 2023, cu aproximativ o oră înainte de furtul ceasului. Acesta a părăsit apoi spitalul după furt, păstrând ceasul asupra sa.

În urma investigației, am reușit să obținem o descriere detaliată a suspectului și am depus un raport la poliție, furnizând toate informațiile pe care le-am strâns. Am luat măsuri suplimentare pentru a îmbunătăți securitatea în zona în care a avut loc furtul.

Concluzie:

În urma investigației, am reușit să identificăm făptașul și am depus un raport la poliție. În plus, am luat măsuri suplimentare pentru a îmbunătăți securitatea în zona în care a avut loc furtul. De asemenea, am recomandat ca personalul să fie instruit în privința măsurilor de securitate și a procedurilor de raportare a incidentelor de acest gen, astfel încât să se poată evita astfel de incidente în viitor.

CAPITOLUL 4

PREVENIREA CRIMINALITĂȚII PRIN PROIECTAREA MEDIULUI ÎNCONJURĂTOR (CPTED)

Acest capitol are o abordare multidisciplinară pentru descurajarea comportamentului criminal prin designul mediului în unitățile sanitare și se concentrează pe patru strategii cheie - controlul natural al accesului, supravegherea naturală, consolidarea teritorială și întreținerea și administrarea proprietății - care pot face unitățile sanitare mai sigure pentru pacienți și personal.

PREVENIREA CRIMINALITĂȚII PRIN PROIECTAREA MEDIULUI ÎNCONJURĂTOR (CPTED)

Crime Prevention Through Environmental Design (CPTED) care se pronunță "sep-ted" este o abordare multidisciplinară pentru descurajarea comportamentului criminal prin designul mediului. Este un instrument esențial în crearea unor medii de sănătate care nu sunt doar vindecătoare și confortabile, ci și sigure.

Standardul "SR ISO 22341:2022 Securitate și reziliență. Securitate preventivă. Ghid pentru prevenirea criminalității prin proiectarea mediului înconjurător" ne spune că CPTED este *"procesul de analiză și evaluare a riscurilor de criminalitate și de securitate pentru a ghida dezvoltarea, proiectarea urbană, gestionarea siturilor și utilizarea mediului construit în vederea prevenirii și reducerii criminalității și a fricii de criminalitate, precum și pentru a promova și îmbunătăți sănătatea publică, calitatea vieții și durabilitatea" cu precizarea că: "designul de mediu se referă la artele și științele aplicate care se ocupă cu crearea mediului proiectat de om."*

Conceptul CPTED este o piatră de temelie în domeniul designului clădirilor unităților sanitare, iar această abordare, care a câștigat recunoaștere globală, utilizează principiile de proiectare ale mediului înconjurător pentru a atenua infracțiunile, pentru a îmbunătăți sentimentul de siguranță și pentru a îmbunătăți calitatea generală a vieții. Interesant este că multe tehnici care îmbunătățesc atractivitatea estetică și integrarea în comunitate a unităților de sănătate contribuie, de asemenea, la prevenirea infracțiunilor.

Infracțiunile, fie că implică atacuri personale, daune aduse proprietății sau prejudicii aduse mediului, apar adesea pentru că oportunitatea există și riscul de detectare este minim sau inexistent. Perspectiva comiterii unei infracțiuni fără a fi observat este un factor descurajant pentru majoritatea potențialilor infractori. Prin proiectarea atentă a mediului fizic pentru a favoriza interacțiunile și vigilența personalului, șansele ca un act infracțional să treacă neobservat pot fi reduse semnificativ. Percepția siguranței este un factor cheie în acest context. Oamenii se îndepărtează în mod natural de zonele pe care le percep ca fiind nesigure, în timp ce zonele active tind să promoveze un sentiment de securitate.

ETAPE CHEIE ÎN CADRUL PROCESULUI CPTED

- ❑ Definiți contextul criminalității și al riscului de securitate
- ❑ Definiți domeniul de aplicare și criteriile
- ❑ Numiți autoritatea responsabilă și echipa de proiect
- ❑ Stabiliți ținta de performanță

- ❑ Identificați activele, amenințările și vulnerabilitățile
- ❑ Identificați cauzele și sursele de risc

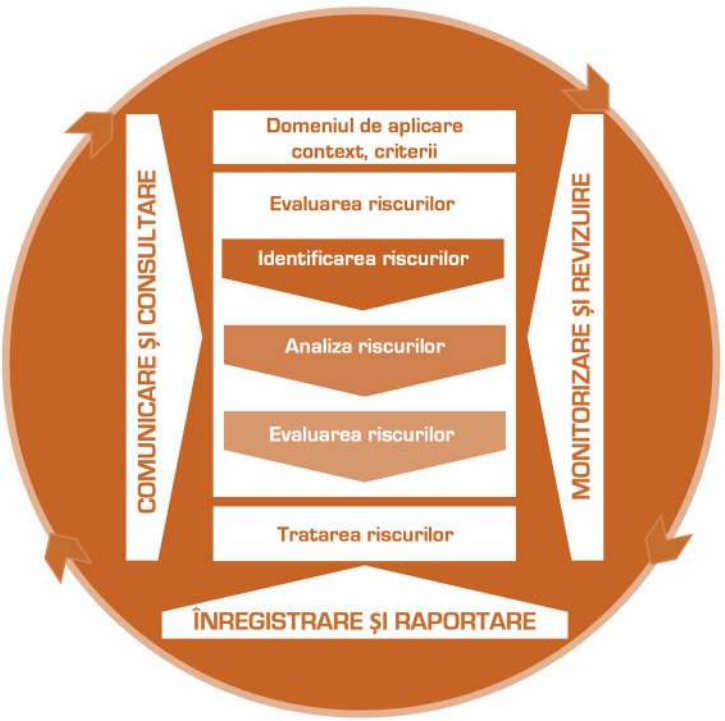
- ❑ Identificați controalele existente
- ❑ Determinați probabilitățile
- ❑ Determinați consecințele
- ❑ Determinați nivelul de risc

- ❑ Comparați criteriile de risc
- ❑ Stabiliți prioritățile strategiilor CPTED

- ❑ Participați cu informații la monitorizarea și revizuirea de către autoritățile de planificare, serviciile de urgență, operatorii de afaceri etc.

- ❑ Identificați opțiunile de tratament
- ❑ Evaluați opțiunile pentru un tratament CPTED personalizat
- ❑ Pregătiți și implementați opțiunile de tratament
- ❑ Analizați și evaluați riscul de criminalitate și securitate rămas

PROCESUL CPTED



STRATEGII CPTED

1. CONTROLUL NATURAL AL ACCESULUI

CPTED cuprinde patru strategii interconectate: controlul natural al accesului, supravegherea naturală, întărirea teritorială și întreținerea și administrarea proprietății.
Implementarea acestor strategii promovează un sentiment proactiv și subtil de siguranță printre vizitatori, personal și pacienți.

Controlul natural al accesului: Această strategie vizează restricționarea și controlul accesului la o proprietate sau facilitate prin designul strategic al intrărilor, ieșirilor, gardurilor, amenajărilor peisagistice și iluminatului. Scopul este de a descuraja accesul neautorizat și de a direcționa vizitatorii de-a lungul rutelor preferate.

CPTED subliniază importanța Controlului natural al accesului ca strategie pentru a descuraja activitățile criminale sau nedorite. Această abordare implică proiectarea strategică a rutelor de acces pentru a ghida pacienții, vizitatorii și uneori personalul, direct către destinațiile lor intenționate, minimizând astfel oportunitățile pentru comportamente negative.

Luăm ca exemplu clinicile ambulatorii. Scopul controlului accesului în spațiile acestora este de a crea un parcurs fără obstacole și direct, pentru pacienți și vizitatori. La intrarea în facilitate, aceștia ar trebui să ajungă imediat la recepție. După programarea lor, ar trebui să se poată deplasa direct către zona de așteptare și apoi să iasă din facilitate fără ocoluri inutile. Acest flux optimizat nu numai că îmbunătățește experiența utilizatorului, dar reduce și potențialul pentru activități infracționale, limitând interacțiunile și expunerile inutile la alte zone ale facilității.

Pentru a realiza acest lucru, este necesară o planificare atentă și o alocare eficientă a spațiului. Zona de parcare destinată clinicilor, de exemplu, ar trebui să fie situată în apropierea imediată a intrării și ieșirii clinicii. Această organizare nu numai că oferă comoditate pentru pacienți și vizitatori, dar contribuie și la siguranța lor. Prin minimizarea distanței pe care trebuie să o parcurgă până și de la vehiculele lor, riscul de incidente în zona de parcare poate fi redus.

În plus, clinica, nu ar trebui să fie ideal situată adânc în interiorul facilității. Necesitatea ca pacienții și vizitatorii clinicii să navigheze prin sau în apropierea departamentelor sau funcțiilor operaționale poate fi nu numai confuză și stresantă pentru ei, dar îi poate expune și la riscuri potențiale.

De exemplu, aceștia pot intra involuntar în zone restricționate sau pot intra în contact cu echipamente, substanțe sau proceduri care ar putea reprezenta un risc pentru siguranța lor. În plus, prezența persoanelor necunoscute ar putea, de asemenea, să perturbe operațiunile acestor departamente și să compromită potențial securitatea lor.

Prin urmare, designul clinicii și al mediului înconjurător ar trebui să aibă ca scop crearea unui traseu clar, direct și intuitiv de la parcare la clinică și înapoi.

Semnalizarea ar trebui să fie clară și suficientă pentru a ghida pacienții și vizitatorii de-a lungul acestui traseu.

Barierele sau caracteristicile peisagistice pot fi utilizate pentru a descuraja subtil devierea de la traseul intenționat. Iluminatul ar trebui să fie adecvat pentru a asigura vizibilitatea și siguranța, în special în timpul orelor de seară.

În plus față de îmbunătățirea siguranței și a securității, această abordare a controlului natural al accesului poate contribui și la o experiență mai plăcută și mai puțin stresantă pentru pacienți și vizitatori.

În concluzie, controlul natural al accesului este o componentă cheie a CPTED, care poate îmbunătăți semnificativ siguranța, securitatea și experiența utilizatorului în unitățile sanitare.

Prin proiectarea atentă a căilor de acces și prin localizarea strategică a facilităților, cum ar fi clinicile ambulatorii, comportamentele nedorite pot fi minimizate, iar calitatea generală a serviciului poate fi îmbunătățită.

STRATEGII CPTED
2. SUPRAVEGHEREA NATURALĂ

Supravegherea naturală este un principiu cheie al CPTED, care subliniază utilizarea strategică a designului fizic pentru a îmbunătăți vizibilitatea și a promova un sentiment de siguranță.

AAbordarea aceasta implică plasarea atentă a ferestrelor, a zonelor deschise și a altor caracteristici pentru a crea linii clare de vizibilitate, descurajând astfel activitățile infracționale potențiale prin reducerea oportunităților de ascundere.

Luăm în considerare exemplul unui spital.

Terenurile și zonele de parcare sunt locații deosebit de importante pentru implementarea supravegherii naturale.

Aceste zone sunt adesea primul punct de contact pentru pacienți, vizitatori și personal, iar siguranța și securitatea lor pot influența semnificativ percepția generală asupra spitalului.

Asigurând linii clare de vizibilitate în aceste zone, pot fi prevenite potențialele agresiuni prin reducerea locurilor de ascundere sau prin protejarea comportamentelor ilegale sau nedorite.

Cu toate acestea, supravegherea naturală nu este doar despre designul fizic. Aceasta implică și promovarea activităților care atrag un număr relativ mare de oameni în zonă pentru funcția sau activitatea desemnată.

Teoria de bază este că o densitate mai mare de oameni face mediul mai puțin atractiv pentru un făptuitor sau un act infracțional.

Prezența altor oameni poate acționa ca un factor descurajant, deoarece potențialii infractori se pot teme de a fi observați sau prinși.

ATENȚIE! Este important de notat că supravegherea naturală nu este o soluție infailibilă.

De exemplu, într-un spital, în ciuda faptului că, cantina funcționa la capacitate maximă la prânz într-o zi de vineri, casierul a fost jefuit cu o armă albă.

Acest incident subliniază faptul că, deși supravegherea naturală poate reduce semnificativ riscul de infracțiune, nu îl poate elimina în totalitate.

Alți factori, cum ar fi îndrăzneala infractorului, prezența personalului de securitate și disponibilitatea indivizilor de a răspunde la o infracțiune în desfășurare, joacă, de asemenea, un rol crucial.

Prin urmare, în timp ce supravegherea naturală este un instrument CPTED valoros, aceasta ar trebui completată cu alte strategii.

De exemplu, spitalele ar putea lua în considerare implementarea măsurilor de control natural al accesului, cum ar fi împrejmuirea strategică sau amenajarea peisajului, pentru a direcționa vizitatorii de-a lungul rutelor preferate și pentru a descuraja accesul neautorizat.

Strategiile de întărire teritorială, cum ar fi semnalizarea clară și facilitățile bine întreținute, pot ajuta, de asemenea, la exprimarea proprietății și la descurajarea potențialilor infractori.

În plus, măsurile de securitate, cum ar fi camerele CCTV, personalul de securitate și sistemele de alarmă, pot oferi straturi suplimentare de protecție.

În concluzie, supravegherea naturală este o strategie puternică pentru îmbunătățirea siguranței și securității unităților sanitare.

Prin proiectarea atentă a mediului fizic și promovarea utilizării active a spațiilor, unitățile sanitare pot descuraja potențialii infractori, pot îmbunătăți sentimentul de siguranță printre pacienți, vizitatori și personal și pot contribui la un mediu de îngrijire a sănătății mai sigur și mai primitor.

STRATEGII CPTED
3. CONSOLIDAREA TERITORIALĂ

Consolidarea teritorială: Această strategie implică utilizarea de atribute fizice care exprimă proprietatea, cum ar fi gardurile, tratamentele pentru pavaj, arta, semnalizarea și amenajarea peisagistică. Aceste caracteristici definesc spațiile publice, semi-publice și private, creând astfel un sentiment de proprietate și responsabilitate printre ocupanți și un sentiment de respect printre cei din afară.

Prin stabilirea unor granițe distincte în cadrul unei unități sanitare sau a unei clădiri din cadrul acesteia, se creează un sentiment de proprietate. Acest lucru transmite un mesaj clar că zonele private sunt rezervate pentru utilizarea și activitatea lor intenționată, descurajând astfel accesul sau activitățile neautorizate. Ideea de bază este de a îmbunătăți subtil percepția unei persoane asupra unei zone ca fiind securizată sau inaccesibilă.

Luăm, din nou, în considerare exemplul unui spital. În cadrul acestuia, există numeroase spații cu diferite grade de acces public și privat - de la holuri și zone de așteptare care sunt deschise tuturor, la saloanele de pacienți și sălile de operație care sunt strict private. Prin definirea clară a acestor spații și a utilizărilor lor intenționate, spitalul poate crea un sentiment de teritorialitate care descurajează accesul sau comportamentul inadecvat.

Implementarea practicilor CPTED, inclusiv întărirea teritorială, este eficientă atunci când este încorporată din faza de planificare a construcției de noi spații, renovării sau relocării funcțiilor. În majoritatea cazurilor, aplicarea principiilor CPTED va necesita diverse măsuri de securitate fizică pentru a completa procesul de control.

Aceste principii sunt universale și au fost adoptate la nivel internațional. De exemplu, Ministerul Justiției din Noua Zeelandă a descris șapte calități pentru locuri mai sigure și bine proiectate, care se aliniază îndeaproape cu principiile CPTED:

1. **Acces: Mișcare și conexiuni sigure** - Acest lucru implică proiectarea căilor și intrărilor pentru a facilita mișcarea sigură și ușoară în întreaga facilitate. Pentru un spital, acest lucru ar putea însemna să aibă intrări și ieșiri bine iluminate, clar marcate și căi accesibile pentru scaunele cu rotile.
2. **Supraveghere și linii de vedere: Vezi și fii văzut** - Acest principiu subliniază importanța vizibilității pentru siguranță. Într-un spital, acest lucru ar putea implica plasarea strategică a posturilor de asistente pentru a supraveghea saloanelor de pacienți sau coridoarele.
3. **Plan: Orientare clară și logică** - Acest lucru implică proiectarea facilității pentru a fi intuitivă și ușor de navigat. Pentru un spital, o semnalizare clară și un flux logic de la un departament la altul pot reduce confuzia și pot îmbunătăți siguranța.
4. **Mix de activități: Ochi pe stradă** - Acest principiu încurajează prezența oamenilor într-o zonă pentru a descuraja activitatea infracțională. Într-un spital, acest lucru ar putea însemna să aibă voluntari sau personal prezent în zonele publice.
5. **Sentiment de proprietate: Arătând că un spațiu este îngrijit** - Acest lucru implică întreținerea bine a facilității pentru a arăta că este îngrijită, ceea ce poate descuraja vandalismul și alte infracțiuni.
6. **Medii de calitate: Medii bine proiectate, gestionate și întreținute** - Acest principiu subliniază importanța unui mediu bine întreținut și gestionat în promovarea siguranței.
7. **Protecție fizică: Utilizarea măsurilor active de securitate** - Acest lucru implică utilizarea măsurilor de securitate fizică, cum ar fi camerele CCTV, personalul de securitate și sistemele de control al accesului, pentru a îmbunătăți siguranța.

În concluzie, prin definirea clară a spațiilor publice și private, promovarea unui sentiment de proprietate și implementarea măsurilor de securitate adecvate, unitățile sanitare pot descuraja activitățile neautorizate, pot îmbunătăți sentimentul de siguranță printre pacienți, vizitatori și personal și pot contribui la un mediu de îngrijire a sănătății mai sigur și mai primitor.

STRATEGII CPTED
4. ÎNTREȚINEREA ȘI ADMINISTRAREA PROPRIETĂȚII

Întreținerea și administrarea proprietății subliniază importanța întreținerii proprietăților pentru a preveni degradarea și vandalismul, care pot semnala o lipsă de control și de grijă, atrăgând astfel activitatea criminală. Întreținerea regulată și repararea rapidă a daunelor pot ajuta la descurajarea potențialilor infractori, indicând o administrare activă și o grijă pentru proprietate.

Prin integrarea acestor strategii în designul unităților sanitare, putem crea medii care nu numai că descurajează infracțiunile, dar promovează și un sentiment de siguranță și bunăstare printre toți utilizatorii. Această abordare contribuie, prin urmare, la obiectivul mai larg de îmbunătățire a calității vieții pentru toți cei implicați.

Starea unei proprietăți poate influența semnificativ vulnerabilitatea acesteia la activitatea infracțională.

O întreținere slabă sau practici de gestionare indiferente pot semnala o lipsă de preocupare pentru proprietate, făcând-o o țintă ușoară pentru activitatea criminală. În contrast, proprietățile bine întreținute și gestionate eficient pot descuraja potențialii infractori, demonstrând un puternic sentiment de proprietate și grijă.

Atunci când se planifică o nouă construcție sau renovare, este important să se ia în considerare strategiile de minimizare a cerințelor de întreținere. Acest lucru nu numai că asigură întreținerea pe termen lung a proprietății, dar contribuie și la securitatea generală a acesteia.

De exemplu, selecția materialului vegetal ar trebui făcută având în vedere dimensiunea acestuia la maturitate, pentru a minimiza necesitatea tăierii.

Acest lucru poate ajuta la menținerea liniilor clare de vizibilitate și la reducerea potențialelor locuri de ascunzătoare, îmbunătățind astfel supravegherea naturală.

Mai mult, **utilizarea materialelor de calitate, durabile, poate reduce semnificativ cerințele de întreținere.**

Materialele de înaltă calitate sunt mai rezistente la uzură, vandalism și daunele mediului, reducând frecvența și costul reparațiilor.

De asemenea, acestea tind să-și păstreze mai bine aspectul în timp, contribuind la un aspect bine întreținut și îngrijit care poate descuraja potențialii infractori.

Practicile eficiente de gestionare a proprietății sunt la fel de importante.

Inspecțiile regulate, reparațiile prompte și aplicarea consecventă a regulilor și reglementărilor pot ajuta la menținerea stării și securității proprietății.

Managerii unităților sanitare ar trebui să fie proactivi în abordarea oricăror probleme care apar, de la reparații minore la potențiale riscuri de securitate.

În plus, managementul proprietății ar trebui să implice și comunicarea regulată cu ocupanții și utilizatorii proprietății.

Acest lucru poate ajuta la promovarea unui sentiment de comunitate și responsabilitate partajată pentru siguranța și întreținerea proprietății, descurajând în continuare potențiala activitate infracțională.

În concluzie, întreținerea și gestionarea proprietății unităților sanitare joacă un rol critic în prevenirea infracțiunilor.

Prin luarea în considerare a cerințelor de întreținere în etapa de planificare, utilizarea materialelor de calitate și implementarea practicilor eficiente de gestionare, proprietățile pot fi menținute într-o stare bună, îmbunătățindu-le siguranța, securitatea și atractivitatea generală.

CPTED - LISTA DE VERIFICARE SPITALUL "MARIA"

CONTROLUL NATURAL AL ACCESULUI

▪ Identificarea tuturor intrărilor și ieșirilor din spital. **DA** ▪ Verificarea vizibilității indicatoarelor pentru intrări/ieșiri. **DA** ▪ Asigurarea că zonele de acces public sunt separate de zonele de acces privat sau restricționat. **NU** ▪ Evaluarea iluminării la toate punctele de intrare și ieșire pe timp de noapte. **NU** ▪ Există barierelor fizice (de exemplu, garduri, bariere) pentru a ghida fluxul de pacienți și vizitatori? **DA** ▪ Asigurarea că parcările sunt bine delimitate și separate de intrări. **DA**	**Puncte pozitive:** intrările și ieșirile sunt bine identificate; indicatoarele pentru intrări/ieșiri sunt vizibile; există bariere fizice pentru a controla fluxul; parcările sunt bine delimitate și separate. **Zone de îmbunătățire:** zonele de acces public și cele private/restricționate trebuie separate; iluminarea intrărilor și ieșirilor pe timp de noapte trebuie îmbunătățită.

SUPRAVEGHERE NATURALĂ

▪ Verificarea tuturor zonelor de așteptare pentru vizibilitate maximă și posibilități de supraveghere. **DA** ▪ Asigurarea că ferestrele de la etajele inferioare oferă vizibilitate către zonele exterioare. **NU** ▪ Evaluarea zonelor ascunse sau slab iluminate care pot fi potențiale puncte slabe. **NU** ▪ Încurajarea utilizării spațiilor comune pentru activități pentru a crește prezența oamenilor. **NU** ▪ Asigurarea că camerele de supraveghere sunt vizibile și bine plasate. **DA**	**Puncte pozitive:** zonele de așteptare au vizibilitate maximă; camerele de supraveghere sunt bine plasate. **Zone de îmbunătățire:** ferestrele de la etajele inferioare trebuie să ofere vizibilitate către exterior; zonele ascunse sau slab iluminate trebuie evaluate și rectificate; trebuie încurajată utilizarea spațiilor comune pentru creșterea prezenței oamenilor.

CONSOLIDAREA TERITORIALĂ

▪ Verificarea dacă există semne sau simboluri care marchează proprietatea și limitele acesteia. **DA** ▪ Evaluarea amenajării peisagistice pentru a distinge zonele publice de cele private. **NU** ▪ Asigurarea că gardurile sau barierele sunt într-o stare bună și nu oferă acces ușor pentru persoanele neautorizate. **DA** ▪ Promovarea unui sentiment de proprietate prin arta comunitară sau alte inițiative. **NU**	**Puncte pozitive:** există semne sau simboluri care marchează proprietatea; gardurile sau barierele sunt solide și nu permit accesul neautorizat. **Zone de îmbunătățire:** amenajarea peisajului trebuie îmbunătățită pentru a distinge zonele publice de cele private; ar fi benefică promovarea unui sentiment de proprietate prin inițiative comunitare.

ÎNTREȚINEREA ȘI ADMINISTRAREA PROPRIETĂȚII

▪ Inspectarea regulată a iluminării exterioare pentru a asigura funcționalitatea acesteia. **DA** ▪ Verificarea periodică a semnalizării pentru deteriorare sau vechime. **DA** ▪ Menținerea curățeniei și eliminarea graffitilor sau a altor forme de vandalizare imediat. **DA** ▪ Asigurarea unei comunicări eficiente cu personalul spitalului privind responsabilitățile și protocolul de securitate. **NU** ▪ Evaluarea stării fizice a clădirilor și a terenului pentru a identifica și repara deteriorările. **DA**	**Puncte pozitive:** iluminarea exterioară este inspecționată regulat; semnalizarea este verificată periodic; existența unui protocol clar pentru curățenie și pentru eliminarea vandalizării; evaluarea și reparația deteriorărilor clădirilor și terenului se realizează. **Zone de îmbunătățire:** este necesară îmbunătățirea comunicării cu personalul spitalului referitor la securitate.

Recomandări: Pe baza acestei interpretări, se recomandă abordarea punctelor identificate ca **"Zone de îmbunătățire"** și implementarea de soluții adecvate. De asemenea, poate fi util să se organizeze sesiuni de formare pentru personalul spitalului în domeniul securității și să se facă o evaluare periodică a măsurilor de securitate pentru a se asigura că acestea rămân eficiente.

CAPITOLUL 5

SISTEME DE SECURITATE FIZICĂ ȘI MECANO-FIZICĂ

Acest capitol descrie sistemele de securitate fizice și mecano-fizice folosite în unitățile sanitare pentru a proteja pacienții, personalul și proprietatea.

Sunt prezentate diferite tipuri de bariere, garduri, bolarzi, dispozitive de blocare, semnalizare și iluminatul de securitate.

ELEMENTE DE BAZĂ
ALE SECURITĂȚII FIZICE PENTRU UNITĂȚILE SANITARE

Măsurile de securitate fizică sunt o componentă esențială a sistemelor de securitate ale unităților sanitare din întreaga lume.

Cu costurile personalului de securitate la un nivel record și cu avansul rapid al tehnologiei de securitate fizică, nu este de mirare că securitatea fizică a fost o zonă semnificativă de îmbunătățire în ultimele decenii.

Evoluția Securității: De la măsuri tradiționale la componente electronice

Într-o lume în care tehnologia și inovația evoluează rapid, securitatea a devenit un domeniu în care adaptabilitatea și inovația sunt esențiale. Chiar dacă măsurile tradiționale de securitate, precum barierele, alarmele, iluminatul și sistemele de încuiere, au fost și rămân pilonii protecției, avansul tehnologic a adus în prim-plan componentele electronice ale securității.

Componentele electronice ale securității, precum camerele de supraveghere conectate la rețea, sistemele de control al accesului bazate pe biometrie sau carduri inteligente și senzorii avansați, oferă un nivel de protecție și monitorizare care depășește capacitatea măsurilor tradiționale. Acestea pot detecta și alerta în timp real despre orice activitate suspectă, permițând o intervenție rapidă și eficientă.

Scopul principal al acestor inovații în domeniul securității este de a proteja resursele vitale împotriva unei game variate de amenințări. Fie că este vorba de spionaj, unde informațiile confidențiale pot fi furate, sabotaj, care poate perturba funcționarea normală a unei instituții, deteriorare, furt sau chiar pierdere, tehnologia modernă oferă soluții adaptate fiecărei provocări.

Integrarea măsurilor de securitate în unitățile sanitare

În unitățile sanitare, securitatea nu este doar o opțiune, ci o necesitate imperativă. Aceste instituții găzduiesc nu doar pacienți și personal medical, ci și echipamente costisitoare, informații confidențiale și resurse vitale. Prin urmare, asigurarea unei protecții adecvate este esențială.

Majoritatea sistemelor de securitate din aceste unități sunt concepute pentru a funcționa ca un tot unitar, în care fiecare componentă se completează și se sprijină reciproc. Măsurile de securitate fizică, cum ar fi camerele de supraveghere, barierele sau sistemele de control al accesului, nu sunt simple instrumente izolate. Ele sunt integrate într-un sistem complex, care include și alte componente ale programului de securitate, precum software-uri de monitorizare, alarme conectate la centrale sau sisteme de identificare avansată.

Această abordare integrată are multiple avantaje. În primul rând, permite o monitorizare și o reacție mult mai rapidă în cazul unei amenințări. De exemplu, o cameră de supraveghere poate detecta o mișcare suspectă, iar sistemul integrat poate trimite imediat o alertă personalului de securitate sau poate bloca accesul într-o anumită zonă.

Personalul de securitate joacă un rol pivot în acest sistem integrat. Ei nu sunt doar gardieni sau observatori pasivi. Datorită tehnologiei avansate și a formării continue, ei pot monitoriza, analiza și răspunde eficient la diversele componente de securitate fizică. De exemplu, în cazul unei alarme declanșate, ei pot verifica rapid sursa acesteia, evaluând dacă este vorba de o amenințare reală sau de o falsă alarmă, și pot lua măsurile adecvate.

Mai mult, personalul de securitate beneficiază de instruire specializată pentru a interacționa cu pacienții, vizitatorii și personalul medical. Aceasta înseamnă că ei nu doar că protejează unitatea sanitară de amenințări externe, dar contribuie și la crearea unui mediu sigur și confortabil pentru toți cei prezenți.

În concluzie, securitatea în unitățile sanitare nu este o sarcină simplă, ci o operațiune complexă și integrată. Prin combinarea măsurilor de securitate fizică cu tehnologia avansată și cu personalul bine pregătit, unitățile sanitare pot asigura un nivel înalt de protecție, adaptat la specificul și nevoile lor unice

GHID GENERAL
MĂSURI DE SECURITATE FIZICĂ PENTRU UNITĂȚILE SANITARE

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid general privind punerea în aplicare a măsurilor de protecție a securității fizice în cadrul serviciilor medicale, cu principii care indică modul optim de utilizare a acestor măsuri de protecție importante.

Declarație

Unitățile sanitare vor implementa măsuri de securitate fizică pentru a stabili un nivel rezonabil de protecție a persoanelor și a activelor, pentru a spori personalul de securitate, politicile și procedurile de securitate. Deoarece eficacitatea măsurilor de protecție fizică utilizate în cadrul unităților sanitare variază, nu există o formulă unică care să determine un plan adecvat de implementare a securității fizice pentru o anumită unitate.

Intenție

A. Utilizarea tuturor măsurilor de securitate electronice și neelectronice utilizate în cadrul unității sanitare ar trebui să aibă o filozofie de utilizare definită și documentată, care să fie revizuită periodic.
B. Măsurile și îmbunătățirile de securitate fizică sunt cel mai bine implementate după efectuarea unei evaluări a riscurilor de securitate. După un eveniment de securitate, planul ar trebui să fie revizuit, cu modificările necesare.
C. Numărul și tipul de măsuri de securitate fizică utilizate în unitățile sanitare pot varia. Utilizând principiile de prevenire a criminalității prin proiectarea mediului (CPTED) pentru o protecție stratificată, ar trebui să se ia în considerare echipamentele și dispozitivele enumerate mai jos:
    1. Controlul accesului, care include uși, mecanisme de blocare, sisteme de chei, încuietori cu buton, tehnologii de acces electronic și porți.
    2. Supravegherea video care include camere de luat vederi, dispozitive de monitorizare, echipamente de înregistrare și interfoane video.
    3. Alarme de efracție pentru detectarea intruziunilor și a mișcării și aplicații de panică/urgență.
    4. Dispozitive de comunicare incluzând telefonia și comunicațiile radio, echipamente și software de distribuție, stații de urgență și dispozitive de notificare în masă.
    5. Echipamente de control, incluzând gestionarea vizitatorilor și detectarea metalelor.
    6. Dispozitive de protecție a activelor, incluzând echipamente folosite pentru a fixa/asigura, sigilii, instrumente utilizate pentru a marca proprietăți, narcotice, casierii, depozitare arme, seifuri și cutii cu încuietori.
    7. Urmărirea pacienților și a activelor, incluzând protecția bebelușilor, monitorizarea bătrânilor și a pacienților cu risc ridicat (alerte de rătăcire) și etichete RFID.
    8. Utilizarea principiilor CPTED, incluzând garduri și bariere, bolarzi, iluminat și amenajare peisagistică.
    9. Protecții pentru pereți, ferestre și stații de lucru, incluzând ferestrele pentru tranzacții, materiale de vitrare protectoare, sticlă rezistentă la gloanțe și designul spațiului de lucru.
    10. Măsuri de descurajare psihologică care să includă indicatoare de securitate, ghiduri de orientare și vehicule de patrulare de securitate clar marcate.
D. Atunci când este rezonabil posibil, echipamentele și dispozitivele de securitate fizică ar trebui să fie standardizate, planificate și implementate într-o manieră integrată.
E. Echipamentele și dispozitivele de securitate fizică ar trebui să completeze și să susțină planul de securitate și reglementările din cadrul jurisdicției unității sanitare.
F. Ar trebui stabilite politici, proceduri și programe de instruire pentru utilizarea, administrarea și răspunsul la diversele măsuri de securitate fizică implementate în unitatea sanitară.
G. Unitatea sanitară ar trebui să aibă un program de întreținere preventivă, inspecție și testare a tuturor echipamentelor și dispozitivelor de securitate fizică pe o bază periodică.
H. O procedură de raportare completă ar trebui utilizată pentru a descrie cum sunt raportate echipamentele și dispozitivele de securitate defecte până la finalizarea acțiunilor corective.

BARIERELE
ROLUL LOR ÎN SECURITATEA UNITĂȚILE SANITARE

Barierele sunt componente esențiale ale programului de securitate al unei unități sanitare.

Acestea pot fi naturale sau create de om și au rolul de a descuraja, întârzia sau detecta accesul neautorizat.

Barierele pot fi clasificate în trei tipuri: naturale, structurale și operaționale.

Fiecare tip are caracteristicile și aplicațiile sale unice în asigurarea securității unităților sanitare.

Barierele joacă un rol esențial în fortificarea securității unităților sanitare, acționând ca primă linie de apărare împotriva amenințărilor potențiale.

Funcția lor principală este de a descuraja accesul persoanelor neautorizate, de a le întârzia progresul în cazul în care încearcă să pătrundă și de a ajuta la detectarea lor. Importanța barierelor devine evidentă atunci când luăm în considerare natura sensibilă a unui mediu de asistență medicală, unde siguranța pacienților, confidențialitatea și protecția echipamentelor și datelor medicale sunt de o importanță capitală.

Să luăm în considerare exemplul "Royal Adelaide Hospital". Situat la periferia unui oraș plin de viață, spitalul este înconjurat de un amestec de bariere naturale și artificiale. Barierele naturale includ o linie densă de copaci și un mic corp de apă pe o parte a proprietății.

Aceste elemente naturale nu numai că îmbunătățesc aspectul estetic al spitalului, dar acționează și ca elemente de descurajare, făcând dificilă abordarea neobservată a unității de către persoane neautorizate.

Din punct de vedere structural, "Royal Adelaide Hospital" este dotat cu ziduri înalte, porți întărite și un sistem de supraveghere de ultimă generație.

Zidurile și porțile au rolul de a întârzia orice tentativă de acces neautorizat, oferind personalului de securitate timp suficient pentru a răspunde.

Sistemul de supraveghere, cu toată gama sa de camere și senzori, asigură că orice activitate neobișnuită este detectată cu promptitudine.

Barierele operaționale de la "Royal Adelaide Hospital" sunt la fel de importante.

Acestea includ protocoale de securitate, cum ar fi înregistrarea vizitatorilor, cerințele privind legitimațiile de identificare pentru personal și zonele cu acces restricționat din cadrul spitalului.

De exemplu, unitatea neonatală din spital are un sistem de acces biometric, asigurându-se că numai personalul autorizat poate intra.

Această măsură operațională nu numai că descurajează potențialele amenințări, dar oferă și un nivel suplimentar de securitate pentru a proteja pacienții cei mai vulnerabili ai spitalului.

În concluzie, barierele, fie că sunt naturale, structurale sau operaționale, sunt componente indispensabile ale strategiei de securitate a unei unități sanitare.

Prin integrarea acestor elemente, instituții precum cele din exemplul prezentat pot asigura un mediu sigur și securizat pentru pacienții, personalul și bunurile lor.

GARDURILE DE PROTECȚIE
PRIMA LINIE DE APĂRARE A UNITĂȚILOR SANITARE

Gardul servește ca perimetru primar de apărare pentru unitățile sanitare. Nu numai că descurajează accesul neautorizat, dar oferă și o demarcație clară a limitelor proprietății.

Alegerea materialului și a designului gardului trebuie să ia în considerare factori precum locația unității, nivelul de amenințare și cerințele estetice. Întreținerea adecvată și inspecțiile regulate sunt esențiale pentru a asigura eficiența gardului ca măsură de securitate.
Gardurile, care reprezintă adesea prima linie de apărare pentru multe unități, au o importanță deosebită pentru unitățile sanitare.

Rolul său transcende dincolo de o simplă barieră fizică; el simbolizează granița dintre domeniul public și un spațiu care necesită respect, intimitate și securitate.

Să luăm, de exemplu, "Policlinica Maria", situata la marginea unui cartier suburban, la granița cu o zonă comercială aglomerată.

Având în vedere locația sa, policlinica este în mijlocul unui trafic pietonal ridicat, nu doar al pacienților și al familiilor acestora, ci și al trecătorilor și al cumpărătorilor de la piața din apropiere.

Pentru a se asigura că spațiile policlinicii rămân în siguranță și pentru a delimita clar limitele acestuia, a fost instalat un gard.

Alegerea gardului pent a fost o combinație de fier forjat și plasă. Această decizie a fost influențată de mai mulți factori.

Apropierea policlinicii de zona comercială a însemnat un nivel de amenințare mai ridicat, necesitând un material robust precum fierul forjat.

Cu toate acestea, pentru a menține o ambianță deschisă și primitoare, au fost folosite inserții de plasă la intervale, asigurând vizibilitatea, fără a compromite securitatea.

Designul a fost atât funcțional, descurajând potențialii intruși, cât și estetic, completând arhitectura modernă a spitalului.

Cu toate acestea, instalarea gardului a fost doar începutul. **Conducerea policlinicii a înțeles că, pentru, ca gardul să rămână o măsură de securitate eficientă, era esențială întreținerea regulată.** A fost stabilit un program pentru inspecțiile de rutină. Acest lucru a asigurat că orice semne de uzură, rugină sau potențiale breșe au fost abordate cu promptitudine.

În plus, **conducerea policlinicii a angajat amenajări peisagistice de-a lungul gardului**, nu doar pentru înfrumusețare, ci și pentru a descuraja potențialii intruși să încerce să se cațere sau să manipuleze gardul.

În concluzie, în timp ce gardul oferă o barieră de securitate tangibilă pentru unitățile de sănătate, eficiența sa este maximizată atunci când este ales cu atenție și întreținut cu sârguință.

Pentru "Policlinica Maria", gardul lor este mai mult decât o simplă delimitare; este o dovadă a angajamentului lor față de siguranță și securitate.

BOLARZII
PROTEJAREA UNITĂȚILOR SANITARE DE AMENINȚĂRILE VEHICULELOR

Bolarzii, denumiți de obicei stâlpi retractabili, de cele mai multe ori ei sunt metalici fabricați din oțel dar sunt și fixi, construiți din beton care servesc ca o barieră fizică pentru a împiedica vehiculele să intre în anumite zone.

Bolarzii au nevoie de o fundație în pământ, deoarece sunt utilizați în exterior. Ei există în diferite variante: permanenți, mobili și/sau retractabili iar designul lor poate fi atât funcțional, cât și estetic.

Rolul lor este acela de a de a controla și/sau dirija traficul rutier dar mai ales pentru a împiedica accesul vehiculelor. În contextul unităților de asistență medicală, aceștia joacă un rol crucial în protejarea clădirilor, a pietonilor și a bunurilor de potențialele amenințări din partea vehiculelor.

Deși, uneori, trecuți cu vederea, bolarzii joacă un rol esențial în infrastructura de siguranță și securitate a multor unități, în special în domeniul sănătății. Funcția lor principală este de a acționa ca o barieră fizică împotriva amenințărilor legate de vehicule, dar importanța lor se extinde dincolo de acest lucru.

Vom lua, din nou, ca exemplu un spital situat în zona centrală a unui oraș. Având în vedere că intrarea sa principală este orientată spre o stradă aglomerată, iar departamentul de urgență primește ambulanțe și pacienți pe tot parcursul zilei, gestionarea traficului de vehicule a devenit o preocupare primordială. Spitalul avea nevoie de o soluție care să asigure siguranța pacienților, a personalului și a infrastructurii sale, menținând în același timp un mediu primitor.

Pentru a rezolva această problemă, spitalul a instalat bolarzi în puncte strategice. La intrarea principală, au fost amplasați bolarzi permanenți, creând o zonă rezervată exclusiv pietonilor. Acești stâlpi rezistenți, realizați din beton armat, nu numai că au împiedicat orice acces accidental sau intenționat al vehiculelor în clădirea principală, dar au adăugat și o notă estetică modernă fațadei spitalului prin designul lor.

La intrarea în departamentul de urgențe, au fost instalați bolarzi retractabili din oțel. În timpul orelor de vârf sau în situații care necesită o securitate sporită, acestia pot fi ridicați, controlând astfel fluxul de vehicule și asigurând că numai cele autorizate, cum ar fi ambulanțele, pot avea acces în zonă. În alte momente, aceștia sunt coborâți, permițând un flux de trafic mai fluid.

În plus, și în **zonele de parcare** au fost amplasați bolarzi retractabili. În caz de urgență, acestia pot fi coborâți rapid, permițând o circulație mai rapidă a vehiculelor, în special a vehiculelor de intervenție de urgență.

Proiectarea stâlpilor din acest exemplu nu a vizat doar funcționalitatea. Cu finisaje elegante și iluminat integrat, acestea au adăugat un element arhitectural peisajului, îmbunătățind exteriorul spitalului, îndeplinind în același timp o funcție de protecție esențială.

Aceștia au asigurat siguranța, au gestionat traficul de vehicule și au adăugat un plus de atractivitate estetică, subliniind angajamentul spitalului atât în ceea ce privește securitatea, cât și excelența în design.

ILUMINATUL
DUBLUL ROL ÎN SECURITATEA UNITĂȚILOR SANITARE

Iluminatul exterior în unitățile sanitare are două scopuri principale: siguranța și securitatea. În timp ce iluminatul de siguranță asigură circulația în siguranță în exterior, iluminatul de securitate descurajează activitatea infracțională, ajută la supraveghere și sporește sentimentul de siguranță personală.

Selectarea, proiectarea și întreținerea corespunzătoare a sistemelor de iluminat sunt esențiale.

Factori precum vandalismul potențial, frunzișul copacilor și tehnologiile de iluminat în evoluție ar trebui să fie luați în considerare pentru a asigura un iluminat eficient în scopuri de securitate.

Iluminatul exterior în unitățile sanitare este mai mult decât o simplă cerință funcțională; este o componentă strategică care are un impact semnificativ atât asupra siguranței, cât și asupra securității.

Reluăm exemplul **"Royal Adelaide Hospital"** un campus spitalicesc ce se mândrește cu grădini frumos amenajate, alei sinuoase și o serie de clădiri interconectate. Pe măsură ce soarele apune, importanța iluminatului exterior devine evidentă.

Pentru siguranță, spitalul dispune de lumini care luminează aleile, asigurându-se că pacienții, vizitatorii și personalul pot circula pe teren fără a se împiedica sau a întâmpina obstacole.

Parcările au lumini situate la înălțimi conforme, asigurându-se că persoanele își pot găsi în siguranță vehiculele.

Toate aceste lumini sunt esențiale pentru a preveni accidentele și pentru a se asigura că toată lumea se poate deplasa în siguranță în incintă.

Din punct de vedere al securității, "Royal Adelaide Hospital" folosește un iluminat strategic în jurul perimetrului clădirilor, în apropierea intrărilor și în alte zone vulnerabile.

Aceste lumini acționează ca elemente de descurajare pentru potențialii intruși, făcând dificilă apropierea persoanelor neautorizate de clădiri fără a fi observate. În plus, camerele de securitate instalate in incinta spitalului beneficiază de această iluminare, capturând imagini mai clare pe timp de noapte, ceea ce ajută la supraveghere.

Cu toate acestea, proiectarea acestui sistem de iluminat nu a fost simplă. **Conducerea spitalului a trebuit să ia în considerare potențialul vandalism**. Astfel, au optat pentru corpuri de iluminat "anti-vandal" în zonele accesibile publicului.

Copacii frumoși, care au contribuit la ambianța senină a spitalului, au reprezentat o altă provocare. Frunzișul arunca deseori umbre sau bloca luminile, astfel încât tăierea regulată a devenit esențială pentru a menține o iluminare eficientă. În plus, odată cu apariția noilor tehnologii de iluminat, spitalul a trecut la lumini LED. Acestea nu numai că, consumă mai puțină energie, dar oferă și o iluminare mai puternică și mai consistentă, sporind atât siguranța, cât și securitatea personalului și a pacienților..

În concluzie, pentru orice unitate sanitară, iluminatul exterior trebuie să fie un amestec armonios de siguranță și securitate.

Luând în considerare provocări precum vandalismul, obstacolele naturale și valorificând tehnologiile în evoluție, unitățile sanitare vor putea asigura un mediu bine iluminat, sigur și securizat pentru toți ocupanții lor.

ILUMINATUL EFICIENT
RECOMANDĂRI

Pentru a menține un program de iluminat eficient, este esențial să prioritizăm siguranța, să descurajăm infracțiunile și să sporim sentimentul general de securitate în cadrul campusurilor unităților sanitare.

Pentru a atinge aceste obiective, managerii de securitate ai unităților sanitare ar trebui să implementeze un set de tehnici directe care, nu numai că vor optimiza investiția în programele de iluminat exterior, dar vor permite și o gestionare adecvată.

Iată câțiva pași cheie de luat în considerare:

Atribuiți un număr unic fiecărui corp de iluminat. O provocare comună este că problemele de iluminat adesea rămân nerezolvate și neraportate.

Acest lucru se datorează parțial faptului că personalul de întreținere lucrează de obicei în timpul zilei, în timp ce problemele sunt predominant observate noaptea.

Pentru a aborda această problemă, este imperativ să simplificăm procesul de raportare pentru toți membrii personalului, inclusiv pentru personalul de securitate.

Acest lucru poate fi realizat etichetând vizibil fiecare lumină exterioară cu o etichetă distinctă, indicând numărul său corespunzător.

Pentru a simplifica și mai mult procesul, creați o hartă cuprinzătoare care să prezinte locația fiecărei lumini, alături de detalii esențiale precum tipul de lampă, puterea, numărul de model, cerința balastului și piesele critice de înlocuire.

Efectuați verificări regulate ale iluminatului atât în timpul zilei, cât și seara. Verificările de zi sunt oportunități valoroase pentru a identifica cauzele secundare ale problemelor de iluminat.

De exemplu, lentilele decolorate pot reduce semnificativ eficiența iluminatului sau corpurile de iluminat stricate ar putea împiedica funcționalitatea corespunzătoare.

Pe de altă parte, verificările nocturne permit detectarea consecințelor reale care decurg din aceste probleme.

De exemplu, acestea ajută la identificarea becurilor arse sau a conflictelor de iluminat rezultate din coroanele copacilor care au crescut prea mult.

- **Identificați zonele care necesită un tratament special de iluminat**, cum ar fi holurile de intrare, departamentele de urgență, punctele de intrare și ieșire a personalului, farmaciile și parcările.
- **Iluminatul de securitate ar trebui să fie activat și dezactivat în mod automat** la ore sau niveluri de lumină prestabilite și să fie conectat la o sursă de alimentare de rezervă, cum ar fi un generator sau un UPS.
- **Iluminatul ar trebui să ofere suficientă luminozitate** pentru a descuraja infracțiunile, a preveni accidentele și a susține camerele de supraveghere.
- **Asigurați-vă că modificările aduse iluminatului nu au un impact negativ asupra performanțelor camerelor de supraveghere**.
- **Iluminatul exterior trebuie să fie adecvat zonei iluminate** fiind în măsură să elimine zonele întunecate și, foarte important, lămpile să fie instalate în carcase rezistente la vandalism și montate astfel încât să împiedice manipularea de persoane neautorizate.
- **Lămplie exterioare și nu numai acestea trebuie să fie întreținute prin mentenanță programată**, inclusiv prin curățarea regulată în timpul primăverii și al verii, deoarece iluminatul poate fi serios împiedicat de insecte.
- **Iluminatul interior** trebuie să contribuie la siguranța și să descurajeze furtul, o parte din acesta trebuind să rămână aprins pe timpul nopții și/sau să fie disponibil prin intermediul senzorilor de mișcare.
- **Semnele de iluminat de urgență/semnele de ieșire în caz de incendiu** trebuie să funcționeze și să nu fie ascunse sau obturate de obstacole, de orice fel.
- **Iluminatul parcărilor** trebuie să contribuie la siguranță și să descurajeze furtul și vandalismul iar în cazul în care unitatea sanitară nu dispune de o parcare dedicată în incintă, trebuie să aibă loc consultări cu autoritățile locale cu privire la iluminatul stradal atunci când sunt identificate pericole/riscuri.

Respectând aceste recomandării, managerii de securitate din unitățile sanitare pot monitoriza și menține eficient programele lor de iluminat, ducând la o securitate sporită, reducerea infracțiunilor și un sentiment general crescut de securitate în cadrul campusurilor facilităților de sănătate.

DISPOZITIVE DE BLOCARE
ÎNCUIETORI ȘI CHEI ÎN UNITĂȚILE SANITARE

Dispozitivele de blocare, respectiv de încuiere, fie tradiționale, fie electronice, sunt esențiale pentru toate sistemele de securitate și îndeplinesc două funcții principale: întârzierea compromiterii securității și furnizarea de dovezi ale intrării forțate. Administrarea corectă a sistemelor de încuietori și chei este esențială pentru securitate.

Multe unități sanitare utilizează, din nefericire, sisteme de încuietori și chei de calitate inferioară din cauza bugetelor alocate dar chiar și atunci când se fac investiții considerabile în echipamente de încuiere performante, ele nu sunt utilizate corespunzător.

Rezistența fizică a unei încuietori determină cât timp este necesar pentru a o învinge prin forță, oferind timp prețios pentru un răspuns. **Încuietorile de înaltă calitate** necesită, unelte și abilități speciale, descurajându-i pe oportuniști. În cazul în care se recurge la forță, rămân dovezi vizuale, cum ar fi feroneria spartă, semnalând o încălcare a securității.

Administrarea corectă a sistemelor de încuietori și chei este, prin urmare, esențială pentru menținerea securității. Politicile stricte de control al accesului ar trebui să dicteze cine poate deține chei și în ce condiții iar inventare stricte trebuie să urmărească toate cheile. Cheile trebuie să fie emise individual și să necesite returnarea, evitându-se astfel o potențială duplicare; auditurile periodice confirmă că toate cheile sunt contabilizate.

Pe scurt, încuietorile fiabile, împreună cu administrarea diligentă a cheilor asociate, asigură un control al accesului pe mai multe niveluri. Asigurarea unei custodii stricte a cheilor, și gestionarea activă a sistemului sunt esențiale pentru securitatea și siguranța unităților sanitare.

Sistemele de încuietori cu miezuri interschimbabile permit schimbarea rapidă a încuietorilor individuale prin schimbarea rapidă a miezurilor modulare.

www.locksmithledger.com

Încuietorile cu miez interschimbabil se recomandă în cazul în care fac parte dintr-un sistem de chei principale de mari dimensiuni sau dacă se preconizează înlocuiri frecvente ale cheilor. În afară de cheile de operare a încuietorii, este necesară o cheie de control pentru a scoate miezul în vederea reîncuietorii sau a service-ului. Recomandăm numirea unei persoane care să fie responsabilă de păstrarea cheii de control și de urmărirea locului în care este utilizat fiecare miez.

În cele mai multe cazuri, atunci când este indicată utilizarea de încuietori cu miezuri interschimbabile, trebuie comandate mai multe miezuri decât cele necesare la început. Acest lucru permite persoanei responsabile să schimbe miezurile atunci când și după cum este necesar. De exemplu, conducerea unui spital ar putea dori să utilizeze încuietori cu miez interschimbabil pentru fiecare unitate din componența sa. Dacă fiecare unitate are o intrare cu cheie în față și în spate, persoana responabilă poate avea la îndemână perechi suplimentare de miezuri, astfel încât încuietorile oricărei unități să poată fi schimbate fără a aștepta mai întâi să vină un lăcătuș, de exemplu.

ATENȚIE! Miezurile interschimbabile permit modificări flexibile ale accesului și o blocare rapidă în cazul pierderii cheilor.

Sisteme de chei principale - cheile selectate pot deschide un număr de uși predefinite. Acesta ajută la menținerea unui control mai bun, economisește costurile de înlocuire a cheilor și este convenabil, deoarece există un număr mai mic de chei în circulație.

Cu toate acestea, sistemele de chei principale care permit ca o singură cheie să deschidă mai multe încuietori sacrifică securitatea în favoarea confortului. Cheile principale reduc combinațiile de chei posibile, iar compromiterea cheii principale distruge mai multe încuietori.

Zonele sensibile, cum ar fi farmaciile, ar trebui să evite cheile principale, în timp ce accesul controlat electronic poate reduce nevoia de chei principale.

DISPOZITIVE DE BLOCARE
ÎNCUIETORI ȘI CHEI ÎN UNITĂȚILE SANITARE

Sistemele computerizate de gestionare a cheilor oferă o urmărire automată a cheilor și a deținătorilor de chei, îmbunătățind responsabilitatea față de înregistrările tradiționale pe suport de hârtie.

Aceste sisteme implică dulapuri inteligente pentru chei care restricționează accesul utilizatorilor autorizați, adesea cu ajutorul cardurilor de acces sau al identificării biometrice. Atunci când cheile sunt scoase, sistemul înregistrează detalii precum numele utilizatorului, cheile împrumutate și ora de ieșire. Cheile sunt blocate în dulap până când sunt eliberate electronic persoanelor autorizate.

Informatizarea evidenței elimină eroarea umană, limitând în același timp accesul fizic. Acest echilibru îmbunătățește securitatea cheilor sensibile și facilitează auditul periodic.

Instalarea corectă a încuietoarelor asigură securitatea. Înlocuirea periodică a încuietorilor asigură o securitate mai mare.

Chiar și încuietorile de înaltă calitate sunt ineficiente dacă sunt instalate necorespunzător. Penetrarea suficientă a zăvorului în cadrul ușii, întărirea corespunzătoare a plăcii de lovire și montarea solidă sunt esențiale. De exemplu, zăvorul ar trebui să intre, cel puțin 2,5 cm în cadrul ușii pentru a preveni atacurile prin pârghie și toate întăriturile ușii trebuie să reziste la încercările de intrare forțată.

Un program permanent, de înlocuire a încuietorilor este optim pentru securitate. Cheile principale la nivelul întregii instalații acumulează rapid chei compromise de-a lungul anilor de rotație a personalului iar încuietorile pentru zonele sensibile ar trebui să fie schimbate la fiecare 3-5 ani și după fiecare incident de securitate.

Deși convenabile, încuietorile cu buton ar trebui limitate la zonele cu risc scăzut, cu excepția cazului în care sunt asociate cu supravegherea video. Acestea sunt cele mai potrivite ca alternativă la cheile fizice pentru personalul general. În concluzie, instalarea corectă, programele de înlocuire ordonată și înțelegerea limitărilor diferitelor tipuri de încuietori contribuie la gestionarea riscurilor.

Dacă sunt instalate corect, lacătele pot oferi o protecție eficientă din punct de vedere al costurilor. Cheile trebuie inventariate periodic pentru a menține responsabilitatea. Restricționarea duplicării cheilor îmbunătățește, de asemenea, securitatea.

Lacătele reprezintă o opțiune economică pentru securizarea magaziilor, a porților, a încăperilor pentru echipamente și a altor zone cu risc scăzut care nu necesită un control avansat al accesului.

Lacătele călite, rezistente la tăiere și forțare, oferă o securitate decentă dacă sunt instalate corespunzător cu zăbrele robuste, fixate cu șuruburi în cadru. Zonele în care se folosesc lacăte ar trebui să aibă totuși o activitate regulată a personalului pentru a descuraja atacurile prelungite și nedetectate asupra încuietorilor.

Trebuie efectuate periodic inventare ale cheilor deținute de personal pentru a se asigura responsabilitatea. Inventarele fizice trebuie să confirme că, cheile corespund cu registrele eliberate.

Restricționarea duplicării cheilor limitează, de asemenea, proliferarea neautorizată. Cheile principale și cele mari ar trebui să fie duplicate numai de lăcătuși calificați, după verificarea autorizației. Cheile pentru zonele de înaltă securitate ar trebui să fie marcate cu ștampila "A nu se duplica", ca mijloc de descurajare.

În concluzie, în mediul dinamic al unităților sanitare, încuietorile, fie ele tradiționale sau electronice, joacă un rol esențial în păstrarea securității.

Este esențială o abordare echilibrată, unde tehnologia modernă complementează metodele tradiționale, pentru a asigura un mediu sigur pentru pacienți, personal și informații.

SEMNALIZAREA DE SECURITATE
ÎN UNITĂȚILE SANITARE

Semnele sunt omniprezente în mediul sanitar, variind ca tip, formă și culoare iar unele dintre ele sunt fundamentale pentru programele de securitate în domeniul sănătății.

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid general privind utilizarea și punerea în aplicare a semnalizării de securitate în unitățile sanitare.

Declarație

Semnalizarea de bază pentru securitate este un element necesar pentru toate unitățile sanitare. Semnalizarea de securitate va fi dezvoltată pentru elementele specifice ale programului de securitate, ghidurile de semnalizare organizatorice și cerințele legale sau regulamentare aplicabile.

Intenție

A. Managerul de Securitate, în colaborare cu conducerea unității sanitare, ar trebui să dezvolte și să mențină semnalizarea de securitate compatibilă cu sistemul general de semnalizare și orientare al facilității.

B. Scopurile principale ale semnalizării de securitate pot fi informative, transmiterea așteptărilor comportamentale, sugestii de sfaturi de securitate sau interzicerea anumitor comportamente sau activități. Un singur semn de securitate poate combina fiecare dintre aceste scopuri principale de securitate. Exemple de semnalizare cu scop principal includ:

Informativ:

- Intrare închisă între 6 p.m. – 6 a.m.
- Intrarea pe timp de noapte pe la Departamentul de Urgență

Așteptări comportamentale:

- Vizitatorii trebuie să se înregistreze
- Mențineți confidențialitatea

Sfaturi de siguranță:

- Verificați obiectele dvs. de valoare
- Încuiați-vă vehiculul

Acte interzise:

- Doar ieșire de urgență
- Această facilitate este o zonă fără arme

C. Respectarea semnalizării de securitate este în general responsabilitatea tuturor angajaților, unității sanitare și nu exclusiv responsabilitatea personalului de securitate. De asemenea, poate exista semnalizare unde conformitatea, poate fi responsabilitatea unui departament, unitate sau funcție a unei poziții atribuite în mod specific.

D. Semnalizarea organizatorică nu poate avea întotdeauna un mesaj specific de securitate, dar poate contribui la obiectivul de a oferi un mediu sigur și securizat. Semnalizarea de securitate poate fi montată, pictată, instalată în pardoseală sau poate fi parte a unei prezentări electronice. Un exemplu este semnalizarea de orientare. Acest tip de semnalizare contribuie la controlul accesului în facilitate, îndrumând direct traficul de vizitatori/pacienți către destinația lor, eliminând astfel rătăcirea, pierderea sau alegerea unor căi care pot crește riscurile de securitate.

E. Semnalizarea de securitate poate fi fixată permanent sau afișată pentru nevoi temporare sau situaționale. Exemple de semnalizare temporară/situațională sunt cele care îndrumă ieșirea în afara orelor de program, instrucțiuni pe termen scurt din cauza proiectelor de construcție, activităților de întreținere sau măsurilor temporare de siguranță a vieții.

F. Situații anticipate, inclusiv semnalizarea pentru gestionarea situațiilor de urgență, care pot fi necesare pentru implementare rapidă (de exemplu, etape de izolare), ar trebui să fie pregătite și depozitate convenabil în avans. Semnalizarea trebuie să fie imprimată astfel încât să reflecte un mesaj profesional, autoritar și ușor de înțeles.

G. Semnalizarea de orientare ar trebui să fie utilizată pentru a orienta și ghida pacienții și vizitatorii către locația dorită. Pentru a fi eficientă, semnalizarea ar trebui să:

- Furnizeze mesaje clare și consistente.
- Utilizeze coduri de culori sau ajutoare de memorie.
- Fie utilizată pentru a crește conștientizarea securității în zonele de parcare, servind în același timp ca descurajare psihologică față de comportamentul criminal și alte comportamente negative.
- Să nu obstrucționeze liniile vizuale naturale.

CAPITOLUL 6

SISTEME DE SECURITATE ELECTRONICĂ

Acest capitol prezintă diferite sisteme electronice de securitate folosite în unitățile sanitare moderne; sisteme de alarmă la efracție, supraveghere video, control al accesului bazat pe carduri sau biometrie, senzori de mișcare și sisteme integrate de management al securității.

Se dau explicații despre cum aceste sisteme pot consolida securitatea fizică, permite monitorizarea în timp real și înregistrarea evenimentelor, restricționarea accesului și detectarea intruşilor evidențiind și importanța integrării și întreținerii adecvate.

MIJLOACE DE PROTECȚIE ȘI DE ALARMARE ÎMPOTRIVA EFRACȚIEI

(CE SPUNE LEGEA DIN ROMÂNIA ...)

LEGEA nr. 333 din 8 iulie 2003 (republicată) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, are următoarele precizări:

Articolul 27

(1) Conducătorii unităţilor care deţin bunuri, valori, suporturi de stocare a documentelor, a datelor şi informaţiilor cu caracter secret de stat sunt obligaţi să asigure paza, mijloacele mecano-fizice de protecţie şi sistemele de alarmare împotriva efracţiei în locurile de păstrare, depozitare şi manipulare a acestora, precum şi în locurile unde se desfăşoară activităţi care au un asemenea caracter.

(2) Proiectele sistemelor de alarmare se avizează de Direcţia Generală de Poliţie a Municipiului Bucureşti ori de inspectoratul de poliţie judeţean pe raza căruia se află obiectivul, sub aspectul respectării cerinţelor minime de securitate împotriva efracţiei.

(3) Elementele de protecţie mecano-fizice încorporate imobilelor destinate păstrării, depozitării şi manipulării bunurilor şi valorilor de orice fel trebuie să fie rezistente la efracţie, corespunzător gradului de siguranţă impus de caracteristicile obiectivului păzit, în conformitate cu cerinţele tehnice stabilite prin normele metodologice de aplicare a prezentei legi.

(4) În sensul prezentei legi, prin elemente de protecţie mecano-fizice se înţelege: ziduri, plase, blindaje, case de fier, seifuri, dulapuri metalice, geamuri şi folie de protecţie, grilaje, uşi şi încuietori.

(5) **În sensul prezentei legi, prin sistem de alarmare împotriva efracţiei se înţelege ansamblul de echipamente electronice care poate fi compus din centrală de comandă şi semnalizare optică şi acustică, detectoare, butoane şi pedale de panică, control de acces şi televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor, corespunzător gradului de siguranţă impus de caracteristicile obiectivului păzit**.

(6) Instalarea, modificarea, inclusiv punerea în funcţiune a sistemelor de alarmare împotriva efracţiei se avizează şi se controlează potrivit prevederilor alin. (2).

(7) Proiectele sistemelor de alarmare împotriva efracţiei se întocmesc în mod obligatoriu pentru obiectivele care sunt supuse avizării poliţiei, iar elaborarea acestora se face cu respectarea cerinţelor tehnice minime stabilite prin normele metodologice de aplicare a prezentei legi.

IMPORTANT!

Toate unitățile sanitare se încadrează la obligativitatea avizării de către poliție a sistemelor de alarmare deoarece fac parte din categoria obiectivelor de interes public și au cerințe minime obligatorii de îndeplinit.

HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003, prevede:

Articolul 67

(1) Asocierea măsurilor şi a mijloacelor de siguranţă prin introducerea mijloacelor mecanofizice de protecţie şi a sistemelor de detecţie, supraveghere şi alarmare se face în baza **analizei de risc la securitatea fizică**.

(2) Deţinătorul sistemelor de supraveghere are obligaţia afişării în unitate a unor semne de avertizare cu privire la existenţa acestora.

(3) Conducătorii unităţilor au obligaţia folosirii mijloacelor de protecţie mecanofizică şi a echipamentelor componente ale sistemelor de alarmare care sunt certificate conform standardelor europene sau naţionale în vigoare de către organisme acreditate din ţară ori din statele membre ale Uniunii Europene sau ale Spaţiului Economic European.

(4) Beneficiarul subsistemului de televiziune cu circuit închis are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, a înregistrărilor video şi/sau audio în care este surprinsă săvârşirea unor fapte de natură penală.

CONSIDERAȚII PRIVIND PROIECTAREA
SECURITĂȚII FIZICE PENTRU UNITĂȚILE SANITARE

Înainte de orice precizări tehnice despre mijloacele de protecție a securității unităților sanitare vrem să subliniem importanța încorporării considerațiilor de securitate în faza incipientă a proiectării unităților sanitare.

Lipsa implicării inițiale a profesioniștilor în securitate poate duce la defecte în proiectare care pot fi costisitoare și perturbatoare pentru corectare și pot compromite siguranța personalului, a pacienților și a vizitatorilor din unitatea sanitară.

Crearea unei unități sanitare sigure necesită un echilibru delicat între preocupările de securitate și diverse alte constrângeri de proiectare, cum ar fi accesibilitatea, costurile, atenuarea pericolelor, protecția împotriva incendiilor, eficiența energetică și estetica.

Prin urmare, departamentul de securitate ar trebui să fie implicat în toate etapele noilor proiecte de construcție și de renovare.

Obiectivul este de a integra fără probleme măsurile de securitate în operațiunile zilnice și în arhitectură, fără a fi intruzive.

Această abordare permite integrarea rentabilă a aplicațiilor de securitate în proiectul general, asigurând un mediu sigur pentru îngrijirea pacienților.

Proiectarea securității trebuie să fie incorporată într-o abordare multirisc, luând în considerare diverse sisteme de construcții, cum ar fi amplasarea, arhitectura, structura, sistemul mecanic și cel electric. Recomandările de securitate oferite ar trebui să formeze baza protecției pentru toate tipurile de unități de sănătate, indiferent de localizarea lor geografică.

Managerul de securitate are un rol vital în influențarea procesului de proiectare și trebuie să se străduiască să participe la toate discuțiile de planificare.

Recomandăm crearea unui "Security Master Plan" desspre care am vorbit anterior sub denumirea de "Planul Strategic de Securitate", (SSP), care să servească drept hartă strategică pentru organizație.

Acest plan ar trebui să includă o viziune de proiectare, utilizarea tehnologiei de securitate care se aliniază la filosofia și obiectivele strategice ale unității și să fie incorporat în proiectarea generală a unității sanitare.

Proiectarea securității ar trebui să fie echilibrată cu obiectivul de a crea un mediu de vindecare confortabil. **Obiectivul este de a asigura că oamenii se simt în siguranță și confortabili, deoarece o vizită la spital poate fi adesea o experiență stresantă**.

GHID PRIVIND INTEGRAREA SISTEMELOR DE SECURITATE ELECTRONICĂ ÎN UNITĂȚILE SANITARE

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid de bază al industriei privind integrarea sistemelor electronice de securitate în mediul medical.

Termenul de "integrare a sistemelor" este utilizat frecvent în discuțiile privind măsurile de protecție prin mijloace electronice. Multe subsisteme sunt achiziționate și întreținute ca tehnologii de sine stătătoare, ceea ce duce adesea la provocări atunci când aceste sisteme trebuie să interacționeze.

Există o tendință din ce în ce mai mare de a proiecta aceste subsisteme multiple pentru a funcționa împreună ca un sistem integrat. Prin urmare, integrarea sistemelor presupune fie operarea subsistemelor de pe o singură platformă, fie coordonarea acestora pentru a obține o monitorizare eficientă și o bună rentabilitate.

Declarație

Unitățile sanitare vor elabora un plan de sistem de securitate electronică pentru a oferi îndrumare și orientare pentru îmbunătățirile existente și viitoare ale sistemului electronic.

Intenție

A. Un sistem electronic de securitate proiectat și instalat în mod corespunzător ar trebui:
   1. Să ofere îndrumări pentru cei implicați în proiectarea sau îmbunătățirea sistemelor de protecție ale unității sanitare (de exemplu, profesioniști în domeniul securității, personal de proiectare și planificare, arhitecți, administratori de unități sanitare).
   2. Să sporească și să îmbunătățească eficiența resurselor de personal
   3. Să descurajeze și să detecteze activitățile infracționale și alte activități nedorite
   4. Furnizează un instrument util de investigare a posteriori

B. Ori de câte ori este posibil, sistemele electronice de securitate ar trebui să fie planificate și implementate într-o manieră integrată. De exemplu: contactele locale ale ușilor sau alte alarme ar trebui să fie integrate cu supravegherea video. Activarea alarmelor ar trebui să se integreze cu sistemele de supraveghere video.

C. Sistemele electronice ar trebui să fie testate, iar rezultatele ar trebui să fie documentate în mod regulat, iar întreținerea ar trebui efectuată în timp util.

D. Punerea în aplicare și îmbunătățirea sistemului de securitate electronică ar trebui să aibă loc după efectuarea unei evaluări a riscurilor de securitate. După un eveniment negativ, planul ar trebui revizuit și, dacă este necesar, ar trebui aduse modificări.

E. Sistemele electronice ar trebui să fie instalate în conformitate cu codurile de siguranță a vieții și de construcție aplicabile. Ar trebui elaborate proceduri de întreținere pentru reducerea potențialului de defecțiuni ale sistemului de alarmă de panică, supraveghere video etc., inclusiv proceduri de testare periodică.

Integrarea se poate extinde dincolo de nivelul de securitate pentru a cuprinde controlul mediului, managementul incendiilor și al energiei. Acest lucru este din ce în ce mai răspândit, în special în spitalele mai mici și în clinicile independente.

Cu toate acestea, există posibilități de monitorizare dublă sau redundantă între sistemele separate de securitate și de gestionare/inginerie a clădirii.

Concluzie: Integrarea tehnologiei de securitate în mediul sanitar necesită o combinație armonioasă de gestionare eficientă a facilităților, de tehnologie a informației (IT) și de cele mai bune practici de securitate actualizate. Fiecare dintre aceste trei componente joacă un rol crucial în securitatea generală și în protecția activelor organizației.

SUBSISTEME DE ALARMARE LA EFRACȚIE
PENTRU UNITĂȚILE SANITARE

HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 are o definiție a subsistemului de alarmare la efracție în Anexa 1, Art.3 (1): "structura subsistemului de alarmare la efracţie este alcătuită din: centrala de alarmă cu tastaturile de operare, elementele de detecţie, echipamentele de avertizare şi semnalizare şi alte componente specifice acestui tip de aplicaţii. Rolul funcţional al subsistemului este de a detecta pătrunderea în spaţiile protejate a persoanelor neautorizate, de a sesiza stările de pericol din unitate şi, după caz, de a îngreuna consumarea actului infracţional."

Pentru a înțelege ce măsuri și ce tip de sistem de alarmare la efracție este potrivit pentru punerea în practică a măsurilor stabilite în „Raportul de evaluare și tratare a riscurilor la securitatea fizică", vă recomandăm să apelați la o companie licențiată de poliție pentru activităţi de proiectare, instalare, modificare sau întreţinere a sistemelor de alarmare împotriva efracţiei.

Sistemele de alarmare la efracție reprezintă o parte esențială a măsurilor de securitate electronică în unitățile sanitare, unde utilizarea lor este în creștere. Atunci când sunt planificate, instalate și utilizate în mod corespunzător, alarmele la efracție pot fi o parte eficientă a unei strategii de securitate proactive, în special dacă sunt încorporate în construcții noi sau în renovări.

Cu toate acestea, adoptarea lor poate fi împiedicată de factori precum limitările de finanțare, lipsa monitorizării în timp real, lacunele de cunoaștere a utilității sistemului, lipsa de acceptare din partea managementului sau a medicilor, problemele percepute sau reale legate de moralul angajaților și lipsa unor abordări inovatoare pentru a asigura finanțarea și implicarea managerului de securitate.

Echilibrul între personalul de securitate și măsurile de protecție fizică este esențial, sistemele de alarmare la efracție fiind concepute în primul rând pentru a spori eficiența personalului de securitate. Aceste sisteme pot reduce potențial numărul de personal de securitate necesar prin creșterea productivității sistemului de securitate.

Alarmele sunt utilizate din ce în ce mai mult pentru siguranța pacienților, cum ar fi alarmele de ușă în unitățile de sănătate comportamentală/mentală sau de îngrijire a persoanelor în vârstă.

Să luăm exemplul unui spital. Așa cum am mai spus, sistemele de sistemele de alarmare la efracție sunt o componentă vitală a oricărui program de securitate al unui spital. Acestea pot fi utilizate pentru a detecta o varietate de amenințări, inclusiv intrări neautorizate și urgențe medicale.

Atunci când sunt instalate și întreținute în mod corespunzător, sistemele de alarmare la efracție pot contribui la menținerea siguranței pacienților, personalului și vizitatorilor.
Există multe tipuri diferite de sisteme de alarmare la efracție care pot fi utilizate în spitale. Unele dintre cele mai comune tipuri includ:

- **Alarme perimetrale:** Aceste alarme sunt folosite pentru a detecta intrarea neautorizată în incinta spitalului. Ele constau de obicei din senzori care sunt plasați în jurul perimetrului proprietății. În cazul în care un senzor este declanșat, o alarmă va suna pentru a alerta personalul de securitate.
- **Alarme de intruziune:** Aceste alarme sunt utilizate pentru a detecta intrarea neautorizată într-o clădire sau într-o cameră. Ele constau, de obicei, din senzori care sunt plasați pe uși, ferestre și alte puncte de acces. Dacă un senzor este declanșat, o alarmă va suna pentru a alerta personalul de securitate.
- **Alarme de urgență medicală:** Aceste alarme sunt folosite pentru a detecta urgențele medicale la pacienți. Ele constau, de obicei, în senzori care sunt plasați pe paturile pacienților sau pe brățările pacienților. În cazul în care un senzor este declanșat, o alarmă va suna pentru a alerta personalul.

În plus față de aceste tipuri comune de sisteme de alarmare la efracție, există o serie de alte sisteme de alarmă specializate care pot fi utilizate în spitale. **De exemplu, unele spitale folosesc sisteme de alarmă pentru a urmări mișcarea bunurilor de mare valoare, cum ar fi medicamentele sau echipamentele medicale**. Alte spitale folosesc sisteme de alarmă pentru a monitoriza comportamentul pacienților care prezintă risc de violență sau de autoagresiune.
Pe măsură ce noi tehnologii devin disponibile, spitalele sunt capabile să implementeze sisteme de alarmă mai sofisticate și mai eficiente. Acest lucru ajută la asigurarea faptului că pacienții, personalul și vizitatorii sunt întotdeauna protejați de orice pericol.

ALARMARE IN CAZ DE CONSTRÂNGERE
(DURESS ALARM SYSTEM) PENTRU UNITĂȚILE SANITARE

În termeni simpli, un "duress alarm system" este un sistem de securitate care permite angajaților să alerteze discret personalul de securitate sau alte autorități atunci când se află într-o situație de urgență sau periculoasă. Dispozitivele pot fi sub formă de telecomenzi portabile, butoane fixate la birou sau senzori de mișcare. În momentul în care sunt activate, acestea trimit un semnal către o stație centrală de monitorizare sau către forțele de ordine, indicând locația exactă a incidentului.

De ce avem nevoie de acest sistem?

Mediul din unitățile sanitare poate fi, din păcate, imprevizibil. De la pacienți agitați până la vizitatori furioși sau chiar potențiali infractori, există multe situații în care am putea avea nevoie de asistență rapidă, fără a atrage atenția.

Exemple de utilizare a "duress alarm system":

Pacient agitat: Un pacient devine violent în camera sa. Ca medic sau asistent, doriți să calmați situația fără a spori tensiunea. Apăsând discret butonul de alarmă, puteți chema securitatea să vină în ajutorul dvs. fără ca pacientul să observe, evitând astfel o escaladare a violenței.

Vizitator supărat: Un vizitator nemulțumit de starea unui pacient sau de timpul de așteptare ar putea să vă abordeze la recepție. Dacă conversația începe să devină amenințătoare, apăsați butonul de alarmă și, în scurt timp, securitatea va fi acolo pentru a gestiona situația.

Situție de urgență în afara orelor de program: Să presupunem că lucrați târziu în noapte și observați o persoană suspectă rătăcind prin coridoarele spitalului. Poate nu doriți să vă confruntați direct cu ea sau să folosiți telefonul, de teamă să nu atrageți atenția. O simplă apăsare a butonului de alarmă vă asigură că securitatea este pe drum.

În sala de urgențe: Personalul medical se confruntă adesea cu situații tensionate. Dacă un pacient sau însoțitorul acestuia devine violent, asistenta medicală poate folosi sistemul de alarmă pentru a alerta securitatea să intervină imediat.

O evaluare a riscurilor de securitate ar trebui să evalueze combinația adecvată de alarme fixe și personale de constrângere și să ia în considerare opțiunile de rezervă în caz de defecțiune a sistemului sau de întrerupere a alimentării cu energie electrică.

Alarmele fixe, cu butoane de alarmare plasate în întreaga unitate sanitară, pot fi alimentate cu baterii sau cablate, în timp ce alarmele personale de constrângere sunt purtate de membrii personalului.

Utilizarea soneriilor de urgență pentru pacienți nu este un substitut acceptabil pentru alarmele fixe sau personale de constrângere iar soluția sistemului de alarmă pentru situații de constrângere trebuie, de asemenea, să țină cont de practicile din întregul campus pentru a se asigura că este eficientă și fără întreruperi.

SUBSISTEME DE CONTROL ACCES
PENTRU UNITĂȚILE SANITARE

HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 are o definiție a subsistemului de alarmare la efracție în Anexa 1, Art.3 (2): "Subsistemul de control al accesului cuprinde unitatea centrală, care gestionează punctele de control, unităţile de comandă, cititoarele, încuietorile sau dispozitivele electromagnetice de acţionare a uşilor, şi are rolul de restricţionare a accesului neautorizat în spaţiile protejate."

Unitățile sanitare, prin natura lor, sunt concepute să fie incluzive și ușor accesibile pentru cei care au nevoie de îngrijire medicală. Deși această intenție de a crea un mediu primitor este esențială, vine cu un dezavantaj. Deschiderea spitalelor, de exemplu, le face, susceptibile la activități criminale și alte pericole potențiale.

Astăzi, unitățile sanitare se confruntă cu un număr tot mai mare de provocări de securitate. Multe spitale, în special cele mai vechi, au numeroase intrări care permit intrarea ușoară pentru pacienți, vizitatori, furnizori și oricine altcineva, uneori, fără o evidență sau o înregistrare adecvată. Această lipsă de control creează o vulnerabilitate care trebuie abordată.

Cheia protejării unei unități sanitare se află în controlul accesului. Acest aspect vital al securității începe cu o considerație atentă a designului facilității și a fluxului de pacienți, vizitatori și personal. Scopul este de a găsi un echilibru între a permite persoanelor să se deplaseze liber fără a se simți restricționați, asigurând în același timp siguranța atât a oaspeților, cât și a angajaților.

Măsurile de control al accesului pot fi implementate pentru a proteja zone critice, cum ar fi farmaciile, sălile de operație și zonele de stocare a tehnologiei, precum și zonele care separă personalul de publicul larg.

Prin restricționarea accesului la aceste zone, nu numai că personalul poate fi mai bine protejat, dar și activele valoroase pot fi, de asemenea, păzite.

Pentru managerii unităților sanitare, este esențial să gestioneze prima impresie pe care pacienții și vizitatorii o au despre facilitate.

Utilizarea sistemelor de control al accesului nu ar trebui să creeze o atmosferă de bariere neprietenoase, în schimb, ar trebui adoptată o abordare gândită pentru a defini și separa clar zonele care sunt deschise publicului de cele care sunt restricționate.

Odată ce aceste zone sunt identificate, se poate determina nivelul adecvat de acces la securitate și mecanismele de blocare.

Măsurile electronice de control al accesului se extind dincolo de simpla deschidere a unei uși.

Acestea permit sau restricționează accesul persoanelor în funcție de cerințele organizației.

Programele software care stau la baza acestor sisteme permit managerilor de securitate să specifice cine are acces, la ce oră și în ce zile sau date specifice. Personalul de securitate sau alte categorii de personal utilizează un software protejat prin parolă pentru alarme sonore de intruziune și generează rapoarte privind activitatea de control al accesului în cadrul instalației. Această activitate poate implica identificarea persoanelor care încearcă să obțină acces în zonele restricționate, precum și identificarea ușilor lăsate deschise sau care necesită întreținere mecanică.

Sistemele electronice de control al accesului de astăzi se pot autoproteja prin solicitarea unei autentificări duble sau triple pentru acces.

Teama de pierdere a cardurilor de identificare este atenuată, deoarece se pot solicita date biometrice sau coduri de identificare personală, împreună cu cardul, pentru a intra în zone cu acces foarte restricționat, cum ar fi farmaciile, depozitele de medicamente și sălile serverelor IT.

Aceste sisteme software pot fi monitorizate de către personalul de securitate într-o cameră securizată, înregistrate pentru referințe ulterioare și utilizate pentru a elabora rapoarte. Alternativ, ele pot trimite o alarmă către un agent de securitate care să intervină în momentul incidentului.

SUBSISTEME DE CONTROL ACCES
MĂSURI ȘI ECHIPAMENTE

Pentru a înțelege ce măsuri și ce tip de sistem de control acces este potrivit pentru punerea în practică a măsurilor stabilite în „Raportul de evaluare și tratare a riscurilor la securitatea fizică", vă recomandăm să apelați la o companie licențiată de poliție pentru activități de proiectare, instalare, modificare sau întreţinere a sistemelor de alarmare împotriva efracţiei.

Specialiștii acestor companii au pregătirea profesională specifică și autoritatea conferită de lege pentru a vă proiecta, instala și întreține sistemele de control acces conform parametrilor proiectați de producătorul echipamentelor.

Măsurile de acces și evacuare trebuie să se concentreze pe deplasarea în siguranță a tuturor persoanelor, angajați, pacienți, vizitatori iar acest lucru implică:

- Identificarea și securizarea perimetrelor clădirilor, inclusiv a ușilor și a ferestrelor, reprezintă un aspect esențial al managementului securității.
- Controlul accesului și ieșirii de pe terenul pe care este situată unitatea sanitară, inclusiv a drumurilor, a serviciilor de urgență, a traficului și a accesului pietonal, a ieșirii și a fluxului.
- Controlul accesului și ieșirii pentru a asigura integritatea perimetrului, de exemplu, alarme pentru uși.
- Asigurarea unui acces și a unei ieșiri sigure, în special după orele de program și în timpul situațiilor de urgență, permite personalului să răspundă și să acceseze retrageri sigure în timp util și în condiții de siguranță.
- Controlul accesului la zonele vulnerabile și securizarea pacienților vulnerabili.
- O orientare clară ajută la asigurarea unei deplasări eficiente și sigure în cadrul unității sanitare.
- Instalarea sistemelor de control/admitere a accesului care permit identificarea persoanelor și limitarea accesului în funcție de cerințele postului sau sarcinii.
- Aplicarea principiile de prevenire a criminalității prin proiectarea mediului (CPTED).

La alegerea celor mai adecvate echipamente de control acces electronice și/sau mecano fizice unitatea sanitară trebuie să ia în considerare o serie de aspecte:

Natura articolelor depozitate în unitatea sanitară: Un spital poate avea o zonă specială unde se păstrează informații sensibile despre pacienți, inclusiv date medicale confidențiale sau rezultate ale testelor. O altă zonă poate fi destinată depozitării medicamentelor controlate, care necesită securitate ridicată din cauza potențialului lor de abuz. De asemenea, zonele de casierie unde se găzduiește numerar sau echipamentele electronice costisitoare, precum RMN-uri, pot fi vizate de hoți.

Necesitatea de a asigura rute de evacuare rapidă: În cazul unui incendiu, cutremur sau a unui incident violent, toți ocupanții unității sanitare trebuie să poată evacua rapid și în siguranță. Asta înseamnă că ușile de ieșire de urgență trebuie să fie deblocate și accesibile, dar, în același timp, protejate împotriva accesului neautorizat din exterior.

Necesitatea de a preveni accesul neautorizat în anumite zone: ExFarmacia din cadrul spitalului poate avea medicamente care pot fi periculoase sau atrăgătoare pentru hoți. Un sistem de carduri de acces sau un sistem biometric poate fi folosit pentru a asigura că numai personalul autorizat poate intra.

Potențialul de utilizare a ieșirilor de urgență: Dacă un hoț intră în clădire și încearcă să fure echipamente sau medicamente, el s-ar putea folosi de ieșirile de urgență, cum ar fi scările de incendiu, pentru a evita să fie prins.

Potențialul de pătrundere prin efracție prin uși și/sau ferestre: Zona administrativă, unde se pot păstra documente valoroase sau echipamente electronice, poate fi vulnerabilă la efracție dacă ferestrele sau ușile nu sunt suficient de securizate.

Potențialul de pătrundere prin efracție și de furt al vehiculelor din parcările interioare: Angajații și vizitatorii pot lăsa bunuri de valoare în vehicule. Parcările interioare trebuie să fie securizate pentru a preveni furtul vehiculelor sau al bunurilor din interiorul acestora. Sistemele de supraveghere video și iluminatul adecvat pot fi esențiale pentru a descuraja hoții.

În concluzie, evaluarea corectă a riscurilor și alocarea resurselor adecvate pentru securitatea fiecărei zone este esențială pentru a asigura buna funcționare și protecția pacienților și a personalului.

SUBSISTEME DE CONTROL ACCES

RECOMANDĂRI PENTRU CONTROLUL UȘILOR

Siguranța într-o unitate sanitară este de cea mai mare importanță, nu doar pentru protejarea pacienților, ci și a personalului medical. Ușile reprezintă unul dintre punctele cheie ale unei astfel de instituții, iar gestionarea lor adecvată poate influența în mod semnificativ securitatea clădirii.

ATENȚIE! Exemplele următoare se referă la denumiri de unități sanitare ipotetice iar orice asemănare cu realitatea este doar o întâmplare.

Accesul exterior limitat se referă la controlul și restricționarea accesului persoanelor prin ușile care duc direct către exteriorul clădirii clinicii. Acest lucru este foarte important, în special seara sau pe timp de noapte, pentru a preveni intrările neautorizate și pentru a asigura securitatea pacienților, personalului și echipamentelor.

Gândiți-vă la acest concept ca la modul în care v-ați încuia casa sau apartamentul pe timp de noapte sau când plecați. Doar pentru că avem o ușă, nu înseamnă că oricine ar trebui să poată intra oricând dorește.

Exemplu: Clinica pediatrica Sunshine. Această clinică, situată într-un cartier rezidențial, are două intrări: una principală și una laterală. Pe timpul zilei, ambele uși sunt deschise pentru a facilita accesul pacienților și vizitatorilor. Cu toate acestea, după ora 20:00, ușa laterală este încuiată și toată lumea este îndrumată să folosească intrarea principală. Astfel, recepționera sau agentul de securitate pot monitoriza și controla cine intră sau iese din clinică pe timp de noapte.

Prin limitarea accesului exterior, clinica asigură un mediu controlat, în care personalul medical poate oferi îngrijiri fără a fi îngrijorat de potențialele amenințări externe sau de perturbări.

Sisteme de avertizare. Într-o unitate sanitară, aceste sisteme sunt folosite pentru a detecta orice încercare de intrare neautorizată prin ușile controlate electronic.

Exemplu: Clinica cardiologica HeartCare. Aici, fiecare ușă care duce către sălile de operație sau laboratoare este dotată cu o încuietoare electronică ce necesită un card de acces. Dacă o persoană încearcă să deschidă acea ușă fără un card valid, un semnal sonor se declanșează la postul de securitate și o lumină roșie se aprinde pe panoul de control, atrăgând atenția asupra încercării de intrare neautorizată.

Implementând astfel de sisteme de avertizare, clinica se asigură că orice tentativă de acces neautorizat este rapid detectată și adresată, protejând astfel atât pacienții, cât și resursele clinicii. Aceasta este o măsură esențială pentru a menține un mediu de lucru sigur și eficient pentru toți angajații.

Interfon și precauție sporită. Un "interfon" este un dispozitiv de comunicare care permite angajaților să audă și/sau să vadă persoana care dorește să intre în unitatea sanitară, înainte de a-i permite accesul.

"Precauția sporită" se referă la măsurile suplimentare pe care le luați pentru a vă asigura că persoanele care intră în unitatea sanitară sunt cele care pretind că sunt și nu prezintă un risc pentru pacienți sau personal.

Exemplu: Spitalul de psihiatrie MindEase. Din cauza naturii tratamentelor și a sensibilității unor pacienți, securitatea este esențială. La intrarea principală, după orele de program, există un sistem de interfon video. Când cineva dorește să intre, trebuie să se identifice vizual și să menționeze motivul vizitei. Personalul de la recepție poate decide să permită accesul sau să ceară asistență de la security înainte de a permite intrarea. Acest lucru asigură că pacienții și personalul sunt protejați de potențialele perturbări sau amenințări.

Prin folosirea interfoanelor și a precauției sporite, clinica se asigură că are un control mai bun asupra persoanelor care intră și ies, reducând astfel riscurile asociate cu intrările neautorizate și creând un mediu de lucru și de tratament mai sigur pentru toți.

Acces restricționat. Într-o unitate sanitară, acest principiu înseamnă că anumite zone, cum ar fi zonele de tratament sau laboratoarele, sunt off-limits pentru public sau chiar pentru anumiți angajați. Aceasta nu se datorează secretomaniei, ci securității: pentru a proteja pacienții, echipamentele și informațiile medicale sensibile.

Exemplu: Clinica de eeurologie BrainTrust. Aici, există un laborator avansat unde se realizează cercetări cu tehnologie de ultimă generație și materiale sensibile. Pentru a proteja aceste resurse valoroase, intrarea în laborator este posibilă doar cu un card de acces special. Chiar și în cadrul personalului clinicii, doar cercetătorii și medicii implicați direct în acele proiecte au un astfel de card.

SUBSISTEME DE SUPRAVEGHERE VIDEO
PENTRU UNITĂȚILE SANITARE

Un sistem de supraveghere video poate fi instalat într-o unitate sanitară pentru a îmbunătăți securitatea pacienților, a personalului și a bunurilor.

Acesta poate fi utilizat pentru a monitoriza activitățile din zona de recepție, a coridoarelor, a parcurilor de mașini, etc. și poate fi utilizat și pentru a detecta și preveni furturile și activitățile ilegale.

HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 are o definiție a subsistemului de alarmare la efracţie în Anexa 1, Art.3 (3): Subsistemul de televiziune cu circuit închis* are în componenţă camerele video, echipamentele de multiplexare, stocare şi posibilitatea de vizualizare a imaginilor preluate, în vederea observării/recunoaşterii/identificării persoanelor.

***NOTĂ!** *Odată cu intrarea în vigoare în 2016 a grupei de standarde **"IEC 62676 Sisteme de supraveghere video utilizate în aplicaţii de securitate",** termenul de televiziune cu circuit închis a fost înlocuit cu "sistem de supraveghere video".*

Am precizat deja că **"Unităţile şi instituţiile de interes public trebuie să prevadă sisteme de supraveghere video pe căile de acces, holuri şi alte zone cu risc ridicat, detecţie a efracţiei pe zonele de expunere sau depozitare valori şi control acces, prin personal sau echipamente."** De aici rezultă că, analiza riscurilor la securitatea fizică va conține OBLIGATIVITATEA unității sanitare de a avea supraveghere video rezultată din cerințele LEGII nr. 333 din 8 iulie 2003 (republicată) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor și a normelor de aplicare.

Acest lucru nu este de ajuns pentru a îndeplini toate cerințele legale deoarece, unitatea sanitară, are și obligații legale de respectare a Regulamentului General de Protecția Datelor și a prevederilor punctuale din LEGEA nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a RGPD care, la Art. 5: Prelucrarea datelor cu caracter personal în contextul relaţiilor de muncă, are următoarele precizări:

În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

a) interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;
b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;
c) angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;
d) alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi
e) durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

Pentru o înțelegere mai bună a situațiilor generate de respectarea Regulamentului General de Protecția Datelor am realizat un capitol special denumit: PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIN MIJLOACE VIDEO.

SUBSISTEME DE SUPRAVEGHERE VIDEO
PENTRU UNITĂȚILE SANITARE

Sistemele de supraveghere video au evoluat semnificativ în ultimii ani. Sistemele video mai vechi aveau nevoie de sute de benzi video pentru înregistrarea continuă și necesitau administrare manuală pentru a schimba benzile periodic pe parcursul zilei.

Evidența înregistrărilor era predispusă la erori, iar găsirea unor evenimente specifice pe bandă era consumatoare de timp. Înregistratoarele video digitale (DVR) și camerele video au făcut progrese semnificative în ceea ce privește caracteristicile și funcțiile, profitând de procesele rapide ale calculatorului și de suporturile de stocare de mare densitate pentru a digitaliza, compresa și înregistra video de la camerele analogice și de la cele digitale.

Supravegherea video, controlul accesului și alarmele au multe în comun și adesea lucrează împreună ca un sistem integrat pentru a împiedica intrarea persoanelor neautorizate în zonele securizate, pentru a limita accesul în unitățile pediatric și de îngrijire neonatală și pentru a monitoriza de la distanță zonele critice în scopul reducerii riscului de infracțiuni și incidente de securitate.

De aceea, tot mai multe unități sanitare continuă să crească utilizarea supravegherii video ca parte a planului lor general de securitate. Integrate împreună, tehnologiile ajută la eficientizarea personalului de securitate și, în general, necesită monitorizare și reacție. Unele sisteme de supraveghere video au o filozofie de utilizare destinată numai capturării (înregistrării) imaginilor care urmează să fie utilizate ulterior, dacă este necesar. În aceste sisteme, poate exista sau nu monitorizare live.

DVR-urile și înregistratoarele video în rețea (NVR) au multe avantaje față de tehnologia analogică de înregistrare mai veche.

Video streaming poate fi înregistrat continuu și șters în cicluri de zile, săptămâni sau luni dacă nu apar evenimente de securitate. Dacă apare un incident, indexarea discului și marcajul de timp fac simplă găsirea videoclipului dintr-o anumită dată și oră. În plus, deoarece videoclipul este digitalizat, acesta poate fi exportat și distribuit prin e-mail sau copiat pe CD, DVD sau alte suporturi digitale folosind programe obișnuite de copiere de rezervă a computerului, care sunt larg disponibile.

Pentru activitățile de supraveghere video există mai multe cerințe operaționale iar selecția echipamentelor trebuie făcută în funcție de aceste cerințe. Iată care sunt acestea:

- **Detectare** - abilitatea de a determina dacă o persoană sau un obiect se află în câmpul vizual al camerei.
- **Recunoaștere** - abilitatea de a diferenția și clasifica oamenii și obiectele în câmpul vizual al camerei (de exemplu, bărbat sau femeie, copil sau adult, etc.)
- **Identificare** - abilitatea de a identifica anumite persoane sau obiecte acolo unde sunt prezente în câmpul vizual al camerei. (Ion Iordache, un autoturism marca Audi, etc.).

NOTĂ! Proiectantul sistemului de supraveghere video, are la dispoziție o serie de instrumente eficiente pentru a stabili , de exemplu, dimensiunea unui obiect (țintă) pe ecranul de afișare.

Pentru a înțelege ce măsuri și ce tip de sistem de supraveghere video este potrivit pentru punerea în practică a măsurilor stabilite în „Raportul de evaluare și tratare a riscurilor la securitatea fizică", vă recomandăm să apelați la o companie licențiată de poliție pentru activităţi de proiectare, instalare, modificare sau întreţinere a sistemelor de alarmare împotriva efracţiei.

Specialiștii acestor companii au pregătirea profesională specifică și autoritatea conferită de lege pentru a vă proiecta, instala și întreține sistemele de control acces conform parametrilor proiectați de producătorul echipamentelor.

SUBSISTEME DE SUPRAVEGHERE VIDEO
GHID GENERAL DE UTILIZARE PENTRU UNITĂȚILE SANITARE

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid general privind utilizarea supravegherii video în unitățile sanitare.

Declarație

Unitățile sanitare vor elabora o politică pentru a oferi îndrumări și direcții privind aplicarea, controlul, autorizarea și utilizarea imaginilor video. Supravegherea video este utilizată în general ca instrument de investigare după producerea faptelor și, atunci când este planificată și instalată în mod corespunzător, poate servi ca element eficient de prevenire a infracțiunilor.

Intenție

a. Fiecare unitate sanitară ar trebui să stabilească cerințele privind supravegherea video în instalații și pe terenuri pe baza evaluărilor riscurilor de securitate.

b. Personalul autorizat din incintă ar trebui să aibă posibilitatea de a observa imagini video din zonele publice prin vizionare în direct sau să aibă posibilitatea de a examina imaginile înregistrate pentru investigarea incidentelor.

c. Fiecare unitate sanitară trebuie să dispună de o politică care să reglementeze protecția informațiilor confidențiale și a imaginilor obținute în urma utilizării supravegherii video.

d. Solicitările părților interesate interne, ale forțelor de ordine, ale agențiilor externe sau ale altor persoane pentru o înregistrare de arhivă a imaginilor video ar trebui să fie adresate persoanei responsabile de funcția de securitate și pot fi aprobate dacă cererea este conformă cu politica și standardele corespunzătoare în materie de confidențialitate și cu politica și standardele. (**Precizăm că, în România**, *"Beneficiarul subsistemului de televiziune cu circuit închis are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, a înregistrărilor video şi/sau audio în care este surprinsă săvârşirea unor fapte de natură penală."* - HG301/2012).

e. Persoana responsabilă cu funcția de securitate ar trebui să elaboreze măsuri adecvate pentru a proteja informațiile sau imaginile obținute prin supravegherea video de securitate și să stabilească un proces astfel încât informațiile sau imaginile să fie observate, înregistrate sau împărtășite numai cu persoanele îndreptățite să primească astfel de informații.

f. Supravegherea video poate fi utilizată în unitățile sanitare în scopuri de securitate netradiționale, pentru a include monitorizarea îngrijirii pacienților sau auditarea proceselor sensibile (de exemplu, manipularea numerarului, a materialelor periculoase, a substanțelor controlate și a productivității lucrătorilor). Astfel de sisteme pot fi utilizate pentru educație și formare, observare directă sau alte utilizări similare. Imaginile obținute din astfel de sisteme sau informațiile stocate în cadrul acestora ar trebui să fie limitate și împărtășite numai cupersonalul aprobat. Atunci când este fezabil, sistemele video utilizate ar trebui să fie întreținute de echipe profesioniste. **(Precizăm că, în România,** *"Unităţile sanitare sunt obligate să încheie contracte de întreţinere periodică cu societăţi licenţiate, care să ateste funcţionarea sistemului conform parametrilor tehnici."* - HG301/2012).

g. Utilizarea supravegherii video sub acoperire poate fi autorizată în anumite circumstanțe și sub un control strict de către persoana responsabilă cu funcția de securitate. **(Acest lucru este interzis în România pentru operațiuni de asigurare a securității)**.

h. Nu ar trebui să se permită utilizarea de camere false.

i. La intrarea în instalația în care se utilizează camere de securitate vizibile se poate amplasa un afișaj care să indice prezența echipamentului de supraveghere video**. (Obligatoriu conform L.333/2003 și GDPR)**

j. Atunci când este integrată cu sistemele de securitate (de exemplu, contacte/puncte de alarmă, interfoane sau alte dispozitive), eficacitatea supravegherii video poate fi sporită.

k. Sunt necesare măsuri de protecție a vieții private pentru a se asigura că colectarea de informații cu caracter personal prin intermediul supravegherii video este legală, justificată și că informațiile obținute sunt prelucrate în mod corespunzător.

l. Politica unității sanitare privind supravegherea video ar trebui să identifice o perioadă de păstrare de cel puțin 10 zile pentru imaginile înregistrate sau conform cerințelor agențiilor de reglementare. **(În România se păstrează minim 20 de zile - L.333/2003 și maxim 30 de zile - GDPR)**

m. Supravegherea video este utilizată și în scopuri clinice, educaționale sau de altă natură.

SUBSISTEME DE SUPRAVEGHERE VIDEO

CERINȚE LEGALE PENTRU UNITĂȚILE SANITARE - EXEMPLE DE APLICAȚII

Unităţile sanitare în România trebuie să prevadă, prin lege, sisteme de supraveghere video pe căile de acces, holuri şi alte zone cu risc ridicat.

(HG 301/2012 - Cerinţe minime pe categorii de unităţi)

Sisteme de supraveghere video pe căile de acces

Exemplu: Intrarea principală a spitalului reprezintă prima linie de interacțiune cu pacienții, vizitatorii și personalul.

Tip de cameră: Cameră cu înaltă rezoluție și funcție de zoom.

Utilitate: ***Securitate, fluxul persoanelor***, ***documentare*** *(în cazul unor litigii sau dispute, înregistrările video pot oferi dovezi valoroase pentru clarificarea situațiilor),* ***prevenirea furturilor***.

Exemplul: Parcarea spitalului este unul dintre locurile în care se desfășoară multe activități, de la sosirea și plecarea pacienților, la transferul de echipamente și medicamente. De asemenea, este un loc unde bunurile personale pot fi vulnerabile, și unde pot avea loc diferite tipuri de incidente, de la simple accidente auto la incidente de securitate.

Tip de cameră: Camere cu înaltă rezoluție și senzori de mișcare.

Utilitate: ***Prevenirea și documentarea furturilor***, ***situatii accidentale*** *(accidente auto),* ***siguranța pacienților și angajaților, gestionarea fluxului de trafic, intervenție rapidă în situații de urgență***.

Sisteme de supraveghere video pe holuri

Exemplul: Holul secției de urgențe este una dintre cele mai aglomerate zone ale unui spital. Aici ajung pacienții cu nevoi medicale urgente, iar fluxul constant de oameni, de la pacienți la medici, asistenți și rude, poate crea o atmosferă intensă și stresantă.

Tip de Cameră: Cameră cu unghi larg de vizualizare. Această cameră ar trebui să poată surprinde întregul hol, astfel încât niciun colț să nu rămână nesupravegheat.

Utilitate: ***Monitorizarea securității*** *(identificarea rapidă a situațiilor conflictuale sau agresive),* ***gestionarea fluxului de pacienți, documentarea evenimentelor, prevenirea și monitorizarea furturilor, evaluarea și îmbunătățirea procedurilor***.

Exemplu: Holurile etajelor unde se află paturile pentru pacienți

Aceste holuri sunt, de obicei, destul de liniștite și sunt dedicate pacienților internați, personalului medical și vizitatorilor. Cu toate acestea, ele reprezintă punctele principale de circulație între camere, săli de tratament și alte facilități ale spitalului.

Tip de Cameră: Cameră cu unghi larg de vizualizare și detectare a mișcării. O cameră cu un unghi larg de vizualizare este esențială pentru a acoperi întregul hol, în timp ce detectarea mișcării poate ajuta la economisirea spațiului de stocare, înregistrând doar atunci când există activitate.

Utilitate: ***Siguranța pacienților și personalului, monitorizarea vizitatorilor, prevenirea furturilor sau vandalismului, documentarea evenimentelor.***

Sisteme de supraveghere video pe alte zone cu risc ridicat

Exemplu: Depozitul de medicamente este o zonă în care securitatea și integritatea sunt esențiale. Prin implementarea unui sistem de supraveghere video eficient, spitalul poate proteja atât medicația esențială pentru pacienți, cât și personalul care lucrează în această zonă.

Tip de Cameră: Camera cu rezoluție înaltă, cu detectare a mișcării și cu acces limitat la vizualizare. Este esențial ca această cameră să ofere imagini clare și detaliate, astfel încât să se poată identifica orice persoană care intră în depozit și orice activitate suspectă.

Utilitate: ***Prevenirea furtului*** *(fie că este vorba de personal neautorizat sau de vizitatori, supravegherea video poate identifica rapid orice activitate suspectă),* ***monitorizarea manipulării medicamentelor*** *(camerele de supraveghere pot ajuta la monitorizarea manipulării corespunzătoare a medicamentelor, asigurându-se că protocoalele sunt respectate și că nu există riscuri pentru pacienți),* ***documentarea accesului*** *(supravegherea video poate oferi o înregistrare clară a persoanelor care au accesat depozitul, ceea ce poate fi esențial în cazul unor investigații sau audituri interne),* ***urmărirea inventarului*** *(deși nu înlocuiește sistemele tradiționale de urmărire a inventarului, supravegherea video poate oferi o confirmare vizuală a intrărilor și ieșirilor de stoc),* ***protecția personalului*** *(în cazul unor acuzații sau neînțelegeri, înregistrările video pot proteja personalul de acuzații nefondate și pot oferi o evidență obiectivă a evenimentelor).*

LISTA DE AUDIT A SECURITĂȚII FIZICE

SPITALUL "MARIA"

(exemplu ipotetic)

Spitalul Maria are responsabilitatea de a asigura un mediu sigur și securizat pentru pacienți, vizitatori și personal. Managerul de securitate joacă un rol cheie în coordonarea eforturilor de securitate fizică în cadrul spitalului.

Această listă de verificare servește ca un instrument util pentru a identifica punctele slabe în securitatea fizică actuală a spitalului și pentru a recomanda îmbunătățiri. Rezultatele listei de verificare oferă o imagine de ansamblu asupra stării securității fizice în Spitalul "Maria".

Dacă un anumit punct din listă nu este îndeplinit, acesta reprezintă o posibilă vulnerabilitate care trebuie adresată. În funcție de priorități și resurse, Managerul de securitate va stabili acțiuni de corectare pentru fiecare dintre aceste vulnerabilități.

SITUAȚIA DE VERIFICAT	DA	NU
Asigurarea securității prin sisteme de securitate fizice și mecano-fizice		
Există garduri și/sau bariere în jurul perimetrului spitalului?		
Bolarzii sunt instalați în zonele critice pentru a preveni accesul vehiculelor neautorizate?		
Iluminatul este adecvat pe timp de noapte și acoperă toate zonele perimetrului și ale clădirii?		
Există sisteme de detectare la încercările de efracție (de ex. la încercarea de tăiere a gardului)?		
Asigurarea securității prin paza umană		
Câți agenți de securitate sunt prezenți în diferite ture?		
Există proceduri clare de patrulare și verificare a perimetrului?		
Agenții sunt instruiți în primul ajutor și în gestionarea situațiilor de urgență?		
Există un sistem de comunicare rapidă între agenții și centrul de control?		
Asigurarea securității prin sisteme de alarmare la efracție și jaf armat		
Alarmele sunt funcționale și testate periodic?		
Există un protocol clar de acțiune în caz de declanșare a alarmei?		
Sistemul de alarmă este monitorizat 24/7?		
Asigurarea securității prin sisteme de supraveghere video		
Camerele de supraveghere acoperă toate punctele de intrare/ieșire și zonele critice?		
Înregistrările sunt păstrate pentru o perioadă de timp adecvată?		
Există un protocol de revizuire a înregistrărilor în caz de incidente?		
Asigurarea securității prin sisteme de control acces		
Există un sistem de acces bazat pe carduri/coduri/biometrie pentru angajați?		
Toate ușile și punctele de acces sunt echipate cu sisteme de control al accesului?		
Există o evidență a persoanelor care accesează zonele restricționate?		

CAPITOLUL 7

SECURITATEA LA INCENDIU

Acest capitol tratează acțiunile de apărare împotriva incendiilor la unitățile sanitare cu accent pe prevenirea şi reducere a riscurilor de producere a incendiilor prin diverse strategii.

APĂRAREA ÎMPOTRIVA INCENDIILOR

ÎN UNITĂȚILE SANITARE

Acest capitol nu reproduce legislația specifică din România privind apărarea împotriva incendiilor.

Ne-am concentrat pe strategiile de bază pentru a obține siguranța la incendiu în unitățile sanitare.

În bibliografie, am menționat sursele care ar trebui consultate de managementul unităților sanitare pentru a respecta legislația specifică.

Incendiile reprezintă o amenințare majoră pentru siguranța și bunăstarea oamenilor și a proprietăților. Această amenințare devine și mai pronunțată în contextul unităților sanitare, unde riscurile sunt amplificate datorită naturii specifice a activităților și resurselor găzduite. În aceste instituții, nu numai că viața și sănătatea pacienților și a personalului medical sunt în pericol, dar și capacitatea de a răspunde la urgențe și dezastre este pusă la încercare.

Factori care amplifică riscul de incendiu în unitățile sanitare:

- **Imposibilitatea de auto-evacuare a pacienților:** Mulți dintre pacienții internați în unitățile sanitare nu pot să se auto-evacueze din cauza stării lor medicale sau a altor limitări. Acest lucru face ca procesul de evacuare să fie mai dificil și să necesite mai mult timp și resurse.
- **Prezența substanțelor inflamabile:** Unitățile sanitare sunt deseori dotate cu cantități mari de oxigen, substanțe volatile și medicamente diverse. Acestea pot agrava și accelera răspândirea incendiilor, dar și emite gaze periculoase pentru sănătate.
- **Rolul esențial în răspunsul la urgențe:** Unitățile sanitare sunt adesea în prima linie de răspuns în caz de dezastre și urgențe. Dacă acestea sunt afectate de incendii, capacitatea de răspuns la alte urgențe este grav compromisă.

Importanța pregătirii și prevenirii. În urma provocărilor aduse de pandemia COVID-19 și a incidentelor recente de incendiu în spitale și alte unități sanitare, a devenit evidentă necesitatea adoptării unor măsuri stricte de prevenire și pregătire.

Aceste strategii sunt esențiale pentru a asigura funcționarea optimă a unităților sanitare și pentru a proteja viața pacienților și a personalului.

Strategii de apărare împotriva incendiilor:

- **Evaluarea riscurilor de incendiu:** Este esențial să se efectueze evaluări periodice ale riscurilor de incendiu pentru a identifica și a aborda vulnerabilitățile specifice fiecărei unități sanitare.
- **Instruirea personalului:** Personalul medical și auxiliar trebuie să fie instruit în mod regulat privind procedurile de evacuare, utilizarea echipamentelor de stingere a incendiilor și primul ajutor în caz de incendiu.
- **Dotarea adecvată:** Unitățile sanitare trebuie să fie echipate cu sisteme de detecție și alarmare a incendiilor, sprinklere, hidranți și alte echipamente de stingere a incendiilor.
- **Planuri de evacuare în caz de incendiu:** Fiecare unitate sanitară ar trebui să aibă un plan de evacuare clar și bine definit, care să fie cunoscut de tot personalul și să fie testat periodic.
- **Revizuirea și actualizarea periodică a protocoalelor:** Protocoalele și procedurile de apărare împotriva incendiilor trebuie să fie revizuite și actualizate periodic pentru a răspunde la noile provocări și pentru a integra cele mai bune practici.

În concluzie, apărarea împotriva incendiilor în unitățile sanitare nu este doar o necesitate, ci o responsabilitate esențială.

Protejarea vieții pacienților, a personalului și a resurselor este o prioritate absolută.

Prin adoptarea și implementarea măsurilor adecvate de prevenire și pregătire, putem asigura că unitățile noastre sanitare rămân sigure și funcționale în fața oricăror amenințări.

EVALUAREA RISCURILOR DE INCENDIU ÎN UNITĂȚILE SANITARE

Evaluarea riscurilor de incendiu în unitățile sanitare este un proces vital, care necesită o atenție deosebită și o abordare sistematică. Este imperativ să se efectueze evaluări periodice ale riscurilor de incendiu pentru a identifica și a aborda vulnerabilitățile specifice fiecărei unități sanitare, fie că este vorba de un spital sau de o clinică specializată, cum ar fi una de neurologie.

Spitalul: Un mediu diversificat și dinamic.

Într-un spital, diversitatea departamentelor și complexitatea serviciilor oferite creează un mediu în care riscurile de incendiu sunt variate și în continuă evoluție.

Exemplu: Riscul de incendiu în departamentul de anestezie și terapie

În aceste departamente, utilizarea echipamentelor electrice și a gazelor medicale inflamabile, cum ar fi oxigenul, crește riscul de incendiu.

Evaluarea riscului în aceste zone implică:

- **Identificarea surselor potențiale de aprindere:** Aceasta include verificarea echipamentelor electrice și a instalațiilor de gaze medicale.
- **Implementarea măsurilor preventive:** Acestea pot include instruirea personalului privind manipularea corectă a echipamentelor și substanțelor inflamabile și implementarea unor proceduri stricte de verificare și întreținere a echipamentelor.
- **Elaborarea planurilor de evacuare și intervenție:** Acestea trebuie să fie adaptate specificului departamentului și să fie cunoscute de tot personalul.

Clinica de Neurologie: Specializare și Focalizare

Într-o clinică de neurologie, specificul activităților și focalizarea pe afecțiuni ale sistemului nervos impun evaluarea și gestionarea atentă a riscurilor de incendiu.

Exemplu: Riscul de incendiu în laboratoarele de cercetare neurologică

Laboratoarele de cercetare neurologică folosesc adesea substanțe chimice și echipamente de precizie, care pot reprezenta surse de incendiu.

Evaluarea riscului în aceste laboratoare implică:

- **Identificarea substanțelor și echipamentelor periculoase:** O listă detaliată a tuturor substanțelor și echipamentelor utilizate trebuie să fie întocmită și revizuită periodic.
- **Implementarea măsurilor de siguranță:** Acestea pot include depozitarea corectă a substanțelor chimice, verificarea regulată a echipamentelor și instruirea personalului în utilizarea sigură a acestora.
- **Elaborarea procedurilor de urgență:** Procedurile de evacuare și intervenție în caz de incendiu trebuie să fie clare, bine definite și cunoscute de tot personalul laboratorului. și pentru a integra cele mai bune practici.

Strategii de prevenire:

Pentru ambele tipuri de unități sanitare din exemplele prezentate, strategiile de prevenire a riscurilor de incendiu sunt esențiale. Acestea pot include:

- **Instruirea și conștientizarea personalului:** Personalul trebuie să fie instruit și conștientizat periodic privind riscurile de incendiu și procedurile de urgență.
- **Implementarea sistemelor de detecție și alarmare:** Sistemele de detecție și alarmare a incendiilor trebuie să fie instalate și întreținute corespunzător.
- **Realizarea de exerciții de evacuare:** Exercițiile de evacuare trebuie efectuate regulat pentru a asigura pregătirea personalului și a pacienților în caz de incendiu.

În concluzie, evaluarea riscurilor de incendiu în unitățile sanitare este un aspect vital al managementului siguranței. Identificarea și abordarea proactivă a vulnerabilităților specifice fiecărui mediu sanitar pot preveni tragedii și pot salva vieți.

Fiecare unitate sanitară, indiferent de dimensiune sau specializare, trebuie să acorde o atenție deosebită evaluării riscurilor de incendiu și să implementeze măsuri adecvate de prevenire și protecție.

Astfel, se poate asigura un mediu sigur și protejat pentru pacienți și pentru cei care le oferă îngrijire.

12 PERICOLE DE INCENDIU ÎN UNITĂȚILE SANITARE

1. **Echipamente electrice defecte.** Echipamentele electrice defecte pot provoca incendii în unitățile sanitare. Fără verificări și întreținere regulată, cablurile deteriorate și aparatele defecte devin riscuri semnificative. Într-o astfel de unitate, un scurtcircuit poate afecta viața pacienților și a personalului.

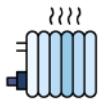
2. **Produse chimice și gaze.** Unitățile sanitare stochează deseori produse chimice și gaze inflamabile. Aceste substanțe, dacă nu sunt gestionate corect, pot provoca incendii devastatoare. Educația și conștientizarea personalului sunt esențiale pentru prevenirea accidentelor grave.

3. **Deșeuri combustibile.** Deșeurile combustibile, cum ar fi ambalajele și materialele de unică folosință, sunt o sursă comună de combustie. Necesită gestionare și depozitare corespunzătoare pentru a preveni posibilitatea unui incendiu și a limita răspândirea acestuia.

4. **Instalații de oxigen.** Instalațiile de oxigen pot fi un pericol major de incendiu în unitățile de sănătate, oxigenul intensificând arderea. Este crucial ca aceste instalații să fie bine întreținute și protejate împotriva scurgerilor și expunerii la surse de căldură.

5. **Blocarea ușilor de evacuare.** Ușile de evacuare și coridoarele blocate cu echipamente sau alte obiecte pot îngreuna evacuarea în caz de incendiu, punând viețile în pericol. Menținerea căilor de evacuare libere este vitală în prevenirea tragediilor.

6. **Echipament medical defect.** Echipamentele medicale defecte sau neîntreținute pot cauza scântei sau supraîncălziri, reprezentând astfel un pericol de incendiu. Este esențial ca acestea să fie inspectate și întreținute regulat pentru a preveni incidente grave.



7. **Lămpi și încălzitoare.** Lămpile și încălzitoarele necorespunzătoare sau plasate incorect pot cauza incendii. Utilizarea responsabilă și amplasarea la distanță de materiale combustibile sunt măsuri critice de prevenție.

8. **Fumatul.** Țigările și alte surse deschise de foc pot fi extrem de periculoase, mai ales dacă sunt lăsate nesupravegheate. Este crucial să se asigure că există zone designete pentru fumat și acestea sunt respectate strict.

9. **Echipamente de gătit.** Echipamentele de gătit defecte sau uitate pe foc în bucătăriile unităților medicale pot provoca incendii rapide. Trebuie implementate proceduri stricte de siguranță pentru prevenirea și controlul acestor tipuri de incendii.

10. **Supraîncărcarea circuitelor electrice.** Supraîncărcarea circuitelor electrice prin utilizarea excesivă de aparate pe aceeași priză poate cauza incendii. Educarea personalului și implementarea unor protocoale stricte sunt esențiale în minimizarea riscului.

11. **Lipsa alarmării la incendiu.** Un sistem de alarmare deficitar sau lipsa acestuia poate întârzia descoperirea și răspunsul la incendii. Instalarea și întreținerea regulată a sistemelor de alarmă de incendiu sunt vitale în detectarea timpurie a incendiilor.

12. **Uleiuri și grăsimi.** Uleiurile și grăsimile pot provoca incendii dacă sunt expuse la temperaturi înalte pentru perioade lungi de timp. Managementul corect al acestor substanțe și monitorizarea echipamentelor de gătit sunt esențiale pentru prevenirea incendiilor.

INSTRUIREA PERSONALULUI ÎN UNITĂȚILE SANITARE

Instruirea personalului din unitățile sanitare în ceea ce privește siguranța împotriva incendiilor este o componentă esențială a managementului riscurilor. Având în vedere complexitatea și diversitatea serviciilor oferite în astfel de instituții, este vital ca fiecare membru al echipei să fie bine pregătit pentru a răspunde eficient și rapid în cazul unui incendiu. **Exemple:**

Spitalul: Un mediu complex cu riscuri diverse.

Într-un spital, diversitatea departamentelor și numărul mare de pacienți fac ca instruirea personalului să fie o provocare, dar și o necesitate absolută.

Exemplu: Instruirea personalului din departamentul de chirurgie.

Într-un departament de chirurgie, riscul de incendiu poate fi amplificat de echipamentele electrice, de substanțele inflamabile și de gazele medicale utilizate. Instruirea personalului în acest context implică:

- **Cunoașterea surselor potențiale de aprindere:** Personalul trebuie să fie conștient de riscurile asociate cu echipamentele și substanțele pe care le utilizează.
- **Utilizarea corectă a echipamentelor de stingere:** Personalul trebuie să știe unde sunt localizate stingătoarele, cum să le utilizeze și să fie instruit în mod regulat prin exerciții practice.
- **Proceduri de evacuare specifice:** Datorită naturii departamentului de chirurgie, unde pacienții pot fi în mijlocul unei intervenții chirurgicale, procedurile de evacuare trebuie să fie adaptate și bine definite.

Centru de sănătate multifuncțional: Diversitate și flexibilitate.

Un centru de sănătate multifuncțional oferă o gamă largă de servicii, de la consultații medicale la terapii alternative. Această diversitate necesită o abordare flexibilă în ceea ce privește instruirea personalului.

Exemplu: Instruirea personalului dintr-un departament de terapie fizică și reabilitare

Într-un astfel de departament, echipamentele electrice și materialele inflamabile pot fi prezente, dar riscul de incendiu poate fi diferit față de alte departamente.

- **Identificarea riscurilor specifice:** Personalul trebuie să fie conștient de particularitățile departamentului și de riscurile asociate.
- **Instruirea în utilizarea echipamentelor de stingere:** Chiar dacă riscul poate fi perceput ca fiind mai mic, personalul trebuie să fie la fel de pregătit să utilizeze echipamentele de stingere.
- **Evacuarea pacienților cu mobilitate redusă:** Procedurile de evacuare trebuie să țină cont de pacienții care necesită asistență sau care nu se pot deplasa rapid.

Elemente comune de instruire:

Indiferent de tipul unității sanitare, există elemente comune de instruire care trebuie abordate:

- **Cunoașterea semnificației alarmelor de incendiu:** Personalul trebuie să știe cum să recunoască alarmele și ce acțiuni să întreprindă imediat.
- **Primul ajutor în caz de incendiu:** Personalul trebuie să fie instruit în acordarea primului ajutor pentru victimele incendiilor, inclusiv în tratamentul arsurilor.
- **Revizuirea și actualizarea periodică a instruirii:** Procedurile, echipamentele și riscurile pot evolua, astfel încât instruirea trebuie să fie un proces continuu.

În concluzie, instruirea personalului medical și auxiliar în ceea ce privește procedurile de evacuare, utilizarea echipamentelor de stingere a incendiilor și primul ajutor în caz de incendiu este esențială pentru siguranța pacienților, a personalului și a întregii unități sanitare.

Prin abordarea proactivă a instruirii și prin adaptarea acesteia la specificul fiecărei unități, se poate asigura un răspuns rapid și eficient în cazul unui incendiu, minimizând astfel riscul de vătămări și de pierderi materiale.

.

DOTAREA ADECVATĂ ÎN UNITĂȚILE SANITARE

Unitățile sanitare găzduiesc nu numai echipamente și resurse valoroase, dar și pacienți și personal care pot fi vulnerabili în fața unui incendiu. Prin urmare, dotarea adecvată a acestor unități cu echipamente și sisteme de protecție împotriva incendiilor este esențială pentru a asigura un mediu sigur și pentru a minimiza riscul de vătămări și pierderi. **Exemple:**

Spitalul de psihiatrie: Un mediu cu provocări specifice.

Un spital de psihiatrie găzduiește pacienți care pot avea dificultăți în a percepe, înțelege și reacționa corespunzător în situații de urgență, cum ar fi un incendiu.

Exemplu: Sistemul de detecție și alarmare a incendiilor într-un spital de psihiatrie.

Într-un astfel de mediu, este vital ca sistemul de detecție și alarmare să fie rapid și eficient. **Acesta trebuie să:**

- **Detecteze rapid orice sursă de fum sau căldură:** Senzorii trebuie să fie amplasați strategic în toate zonele spitalului, inclusiv în camerele pacienților, coridoare și spații comune.
- **Emită alarme auditive și vizuale:** Având în vedere specificul pacienților, alarmele vizuale pot fi la fel de importante ca cele auditive, pentru a atrage atenția și a indica direcția de evacuare.
- **Fie conectat la un centru de supraveghere:** Astfel încât personalul să fie alertat imediat și să poată interveni rapid.

Centrul de diagnostic și tratament: Diversitate și precizie.

Un centru de diagnostic și tratament oferă o gamă largă de servicii medicale, de la imagistică la laboratoare și proceduri chirurgicale minore.

Datorită acestei diversități, dotarea adecvată împotriva incendiilor trebuie să fie bine gândită.

Exemplu: Sistemul de sprinklere într-un centru de diagnostic și tratament.

Un sistem de sprinklere este esențial pentru a controla și limita răspândirea unui incendiu.

Într-un centru de diagnostic și tratament:

- **Sprinklerele trebuie să fie amplasate strategic:** Acestea trebuie să fie prezente în zonele cu echipamente electrice, laboratoare și orice altă zonă cu risc crescut de incendiu.
- **Sistemul trebuie să fie conectat la o sursă de apă fiabilă:** Asigurarea unui flux constant de apă este esențială pentru eficiența sistemului.
- **Verificări și întreținere regulată:** Sistemul de sprinklere trebuie verificat periodic pentru a se asigura că funcționează corect și că nu există blocaje sau defecte.

Echipamentele de stingere a incendiilor: O necesitate universală.

Indiferent de tipul unității sanitare, există echipamente de bază de stingere a incendiilor care trebuie să fie prezente:

- **Hidranți:** Aceștia oferă o sursă rapidă de apă și trebuie să fie amplasați strategic în întreaga unitate sanitară.
- **Stingătoare:** Acestea trebuie să fie ușor accesibile și personalul trebuie să fie instruit în utilizarea lor. Tipul de stingător (CO2, pulbere, spumă) trebuie să fie adecvat riscurilor specifice zonei în care este amplasat.
- **Pături anti-incendiu:** Acestea pot fi utilizate pentru a stinge incendiile mici sau pentru a proteja persoanele în caz de evacuare.

În concluzie, dotarea adecvată a unităților sanitare cu echipamente și sisteme de protecție împotriva incendiilor este mai mult decât o recomandare - este o responsabilitate.

Fiecare unitate sanitară, de la spitalele de psihiatrie la centrele de diagnostic și tratament, trebuie să fie pregătită să răspundă eficient și rapid în cazul unui incendiu.

Prin investiții în echipamente de calitate și prin instruirea continuă a personalului, se poate asigura un mediu sigur pentru pacienți, personal și resurse.

.

PLANURI DE EVACUARE ÎN CAZ DE INCENDIU

În orice instituție, dar mai ales în unitățile sanitare, pregătirea pentru situații de urgență, precum incendiile, este esențială. Un plan de evacuare bine definit și cunoscut de tot personalul poate face diferența între salvarea de vieți și tragedie. Aceste planuri trebuie să fie adaptate specificului fiecărei unități și să fie testate periodic pentru a asigura eficiența lor în caz real. **Exemple:**

Spitalul: Un mediu complex cu multe variabile.

Într-un spital, diversitatea departamentelor, numărul mare de pacienți și complexitatea infrastructurii fac ca planurile de evacuare să fie o provocare.

Exemplu: Planul de evacuare pentru un departament de terapie intensivă.

Într-un departament de terapie intensivă, pacienții sunt adesea în stare critică și depind de echipamente vitale. Evacuarea lor necesită o abordare specială:

- **Căi de evacuare dedicate:** Aceste căi trebuie să fie largi și fără obstacole, pentru a permite transportul rapid al pacienților pe paturi sau în scaune cu rotile.
- **Echipamente de suport vital portabile:** În cazul unei evacuări, echipamentele de suport vital, precum ventilatoarele, trebuie să fie portabile și dotate cu baterii pentru a asigura continuitatea îngrijirilor.
- **Personal instruit:** Personalul trebuie să fie instruit specific pentru evacuarea pacienților critici, știind exact ce echipamente să ia cu ei și cum să asigure suportul vital în timpul evacuării.

Elemente comune în planurile de evacuare.

Indiferent de tipul unității sanitare, există elemente esențiale care trebuie incluse în orice plan de evacuare:

- **Puncte de adunare:** Acestea sunt locuri sigure, în afara clădirii, unde pacienții și personalul se pot aduna după evacuare pentru a fi numărați și evaluați.
- **Comunicare:** Sistemele de comunicare, precum megafonele sau radiourile, sunt esențiale pentru a coordona evacuarea și pentru a transmite informații vitale.
- **Exerciții periodice:** Testarea planului de evacuare prin exerciții periodice este esențială pentru a identifica și corecta eventualele deficiențe și pentru a asigura că toți angajații sunt familiarizați cu procedurile.

Centrul medical ambulatoriu: Flexibilitate și rapiditate.

Într-un centru medical ambulatoriu, numărul pacienților și complexitatea cazurilor pot varia, dar necesitatea unui plan de evacuare rămâne la fel de importantă.

Exemplu: Planul de evacuare pentru un centru medical ambulatoriu cu multiple specialități.

Într-un astfel de centru, pacienții pot fi prezenți pentru consultații, investigații sau proceduri minore. Planul de evacuare trebuie să țină cont de această diversitate:

- **Căi de evacuare clare și semnalizate:** Indiferent de motivul vizitei, pacienții și personalul trebuie să știe cea mai rapidă cale de ieșire. Semnalizarea trebuie să fie vizibilă și ușor de înțeles.
- **Zone de adăpost:** În cazul în care evacuarea completă nu este posibilă sau sigură, trebuie identificate zone în interiorul clădirii unde pacienții și personalul pot fi adăpostiți temporar.
- **Instruirea personalului:** Fiecare membru al personalului trebuie să cunoască planul de evacuare și să fie pregătit să ghideze și să asiste pacienții în caz de urgență.

În concluzie, fiecare unitate sanitară, fie că este vorba de un spital sau de un centru medical ambulatoriu, trebuie să aibă un plan de evacuare clar și bine definit în caz de incendiu.

Aceste planuri nu numai că protejează viețile pacienților și ale personalului, dar și resursele și echipamentele vitale.

Prin planificare, instruire și testare regulată, unitățile sanitare pot fi pregătite să răspundă eficient și rapid în fața oricărei situații de urgență.

REVIZUIREA ȘI ACTUALIZAREA PERIODICĂ A PROTOCOALELOR

Într-un domeniu în continuă evoluție precum cel al sănătății, adaptabilitatea și actualizarea constantă a protocoalelor sunt esențiale pentru a asigura siguranța și eficiența. Acest lucru este cu atât mai important în ceea ce privește protocoalele și procedurile de apărare împotriva incendiilor, unde mizele sunt extrem de ridicate. **Exemple:**

Spital Universitar.

Un spital universitar este adesea la avangarda cercetării și inovației medicale, având un flux constant de noi echipamente, tehnologii și metode de tratament.

Exemplu: Introducerea unui nou echipament de imagistică.

Un nou echipament de imagistică, cum ar fi un RMN de ultimă generație, poate necesita condiții speciale de funcționare, inclusiv răcire cu heliu lichid. Acest lucru poate introduce noi riscuri de incendiu sau explozie.

Revizuirea și actualizarea protocoalelor în acest context ar implica:

- **Evaluarea riscurilor asociate cu noul echipament:** Identificarea surselor potențiale de aprindere și a substanțelor inflamabile.
- **Adaptarea procedurilor de evacuare:** În cazul unei urgențe legate de noul echipament, personalul și pacienții trebuie să știe cum să reacționeze și pe unde să evacueze.
- **Instruirea personalului:** Personalul trebuie să fie instruit în legătură cu noile riscuri și cu modul de utilizare în siguranță a echipamentului.

Un centru de reabilitare.

Un centru de reabilitare se concentrează pe recuperarea pacienților după accidente sau boli grave, având adesea pacienți cu mobilitate redusă sau alte dizabilități.

Exemplu: Renovarea și extinderea spațiilor de terapie.

În urma unei extinderi, centrul dispune de noi spații de terapie, inclusiv o piscină terapeutică și săli de kinetoterapie dotate cu echipamente moderne.

Revizuirea și actualizarea protocoalelor în acest context ar implica:

- **Evaluarea noilor riscuri asociate cu spațiile și echipamentele:** Apa din piscina terapeutică poate reprezenta un risc în combinație cu echipamentele electrice, iar echipamentele de kinetoterapie pot necesita surse de alimentare speciale.
- **Adaptarea planurilor de evacuare:** Pacienții cu mobilitate redusă pot necesita căi de evacuare speciale sau asistență suplimentară.
- **Instruirea personalului:** Personalul trebuie să fie familiarizat cu noile spații, echipamente și potențialele riscuri asociate, și să fie pregătit să asiste pacienții în caz de urgență.

Importanța revizuirii și actualizării periodice.

Indiferent de tipul unității sanitare, există o serie de pași esențiali în procesul de revizuire și actualizare a protocoalelor:

- **Monitorizarea constantă a riscurilor:** Riscurile trebuie evaluate în mod regulat, mai ales după introducerea de noi echipamente, tehnologii sau proceduri.
- **Feedback de la personal:** Personalul, fiind în prima linie, poate oferi feedback valoros privind eficiența protocoalelor existente și potențialele zone de îmbunătățire.
- **Integrarea celor mai bune practici:** Conformarea la standardele naționale și internaționale și adaptarea la cele mai bune practici din industrie pot contribui la creșterea eficienței și siguranței.

În concluzie, revizuirea și actualizarea periodică a protocoalelor și procedurilor de apărare împotriva incendiilor sunt esențiale pentru a asigura un mediu sigur în unitățile sanitare.

Adaptabilitatea și proactivitatea în fața noilor provocări și integrarea constantă a celor mai bune practici sunt cheia pentru protejarea pacienților, personalului și resurselor.

ALARMELE FALSE ÎN DETECȚIA INCENDIILOR ÎN UNITĂȚILE SANITARE

În unitățile sanitare, un sistem eficient de detecție și alarmare la incendiu este vital pentru siguranța pacienților și a personalului. Cu toate acestea, alarmele false pot crea panică, evacuări inutile și pot degrada încrederea în sistem, motiv pentru care este imperativ să se acorde o atenție sporită prevenirii acestora.

Cauzele alarmelor false

Alarmele false în unitățile sanitare pot fi cauzate de:

a. **Lucrări în zonele supravegheate:** Deseori, în spitale au loc lucrări de reparație sau mentenanță. Dacă detectoarele nu sunt dezactivate corespunzător, pot rezulta alarme false.
b. **Condiții ambientale:** Activitățile specifice, ca de exemplu căldură, fum, flăcări, abur sau praf rezultate din gătit sau din procese de producție sau gaze de eșapament de la autovehicule, pot genera alarme false.
c. **Defecte mecanice și electrice:** Vibrațiile de la echipamentele medicale, coroziunea cauzată de dezinfectanți sau impactul cu carucioarele pot afecta sistemul.
d. **Service sau testări:** Alarmele false pot rezulta dacă aceste activități nu sunt comunicate sau coordonate corect. De exemplu: lucrări de service sau încercări efectuate fără înștiințarea prealabilă a brigăzii de pompieri sau a dispeceratului de recepție a alarmei.
e. **Lucrări de service executate incorect.**
f. **Fenomene electrice tranzitorii** (de exemplu descărcări electrice sau variații ale curentului la conectarea unor consumatori) sau interferențe radioelectrice;
g. **Acumularea de praf sau insecte:** În medii curate, cum sunt sălile de operație, pot exista totuși condiții care favorizează acumularea de praf sau insecte.
h. **Modificări ale destinației sau amenajării clădirii:** Reamenajările sau extinderile spitalului, de exemplu, fără ajustarea corespunzătoare a sistemului de detecție pot genera alarme false.
i. **Acționarea accidentală sau cu rea-voință a declanșatoarelor manuale sau a detectoarelor.**

Vulnerabilități ale diferitelor tipuri de detectoare

a. **Detectoare de fum:** Alarmele false semnalizate de detectoare de fum pot fi cauzate de fum sau de alte emanații, praf (incluzând acumulări lente de praf și particule purtate de curenți), fibre, abur sau condens; toate acestea pot fi cauzate de procese sau activități normale sau de condiții de mediu extreme. Infestarea cu insecte poate constitui o problemă semnificativă.
a. **Detectoare de căldură:** În zonele unde aparatele de încălzire sunt folosite intensiv, sau unde razele solare pot lovi direct detectorul, pot exista alarme false.
b. **Detectoare de flacără:** Detectoarele de flacără în spectru ultraviolet detectează radiațiile emise de flăcări în spectrul ultraviolet. Acestea sunt susceptibile a fi declanșate de surse precum descărcările electrice, radiațiile ionizante, lămpile în ultraviolet sau lămpile halogene, dacă sistemul nu poate face distincția între aceste surse, însă nu sunt sensibile la lumina solară (componenta ultravioletă a radiației solare la care detectoarele sunt sensibile este filtrată de stratul de ozon aflat în partea superioară a atmosferei).

Măsuri de prevenire

a. **Detectoare multisenzor:** Combinând diverse modalități de detecție, aceste detectoare pot reduce semnificativ numărul de alarme false.
b. **Semnalizarea prealarmelor:** Pentru a evita evacuări inutile, un sistem de prealarmă poate alerta personalul că există o posibilă problemă. Acest lucru permite investigația rapidă a cauzei și oprirea potențialei alarme false înainte de a genera panică.
c. **Interdependența semnalelor:** Confirmarea alarmei de la două detectoare diferite înainte de a declanșa o alarmă completă poate preveni semnalările eronate.
d. **Sisteme corelate cu activitatea din clădire:** În cazul în care activitatea umană sau industrială pe parcursul zilei sau în perioada de activitate poate genera alarme false, în special acolo unde prezența și obiceiurile comportamentale ale oamenilor fac improbabilă dezvoltarea unui incendiu fără a fi remarcat de utilizatorii clădirii, devine utilă luarea în considerare a unui sistem corelat cu activitatea din clădire. **Exemplu: Confirmare pre-transmisie.** În anumite situații (dar nu în toate), acolo unde există o frecvență ridicată a alarmelor false, care nu poate fi redusă prin alte măsuri, este recomandată întârzierea transmisiei automate a alarmei către brigada de pompieri cu o durată suficient de mare pentru a permite investigarea alarmei.

CAPITOLUL 8

CONSIDERAȚII SPECIALE PRIVIND SECURITATEA ÎN DOMENIUL SĂNĂTĂȚII

Acest capitol tratează acțiunile de prevenirea și gestionare a agresivității și a violenței în sistemul de sănătate, zonele de risc ridicat, zone de interes special, parcarea și mediul extern al unități sanitare.

PREVENIREA ȘI GESTIONAREA AGRESIVITĂȚII ȘI VIOLENȚEI
ÎN UNITĂȚILE SANITARE

Unitățile sanitare, cu toate că sunt create pentru a oferi îngrijire și asistență pacienților, pot fi, uneori, scene ale unor incidente de agresivitate sau violență.

Acestea pot fi declanșate de stres, anxietate, percepții eronate sau de comportamentul inadecvat al unor pacienți sau vizitatori.

Pentru a proteja atât personalul medical, cât și pacienții, este esențial să înțelegem, prevenim și gestionăm aceste situații.

Câteva, din cauzele agresivității în unitățile sanitare:

- **Stresul și anxietatea:** starea de sănătate și incertitudinea prognosticului pot duce la stres și anxietate în rândul pacienților și familiilor lor.
- **Percepții eronate:** unele persoane pot percepe greșit acțiunile personalului medical sau pot simți că nu sunt suficient de bine îngrijite.
- **Probleme psihiatrice sau medicale:** pacienții cu anumite afecțiuni pot avea un comportament agresiv sau imprevizibil.

Metode de prevenire:

- **Formare și educație:** personalul medical ar trebui să primească instruire privind recunoașterea semnelor de agresivitate și tehnici de dezamorsare.
- **Comunicare eficientă:** claritatea și empatia în comunicare pot preveni multe situații tensionate.
- **Securitate fizică:** accesul controlat, camerele de supraveghere și prezența personalului de securitate pot descuraja comportamentele agresive.

Gestionarea incidentelor:

- Evaluarea situației: este esențial să determinați dacă situația este o amenințare imediată sau dacă poate fi gestionată prin comunicare.
- Tehnici de dezamorsare: personalul ar trebui să utilizeze tehnici verbale pentru a calma persoana agitată, evitând confruntarea fizică dacă este posibil.
- Intervenție fizică sau chimică: în situații extreme, se poate recurge la restrângerea fizică a pacientului sau la administrarea de medicamente pentru a-l calma.

Exemplu: La un spital din Timișoara, o vizitatoare a devenit extrem de agresivă după ce i s-a comunicat că nu poate vizita un pacient în afara orelor de vizită.

Folosind tehnici de de-escaladare, personalul de securitate a colaborat cu asistenții medicali pentru a o conduce pe vizitatoare într-o zonă liniștită unde a putut discuta situația și a înțelege regulile spitalului, evitând astfel o confruntare fizică.

Vă prezint două tehnici de de-escaladare pe care personalul de securitate le-a utilizat în această situație:

Comunicarea activă și empatică: Personalul de securitate poate folosi tehnici de comunicare empatică pentru a demonstra vizitatoarei că ei înțeleg frustrarea și dezamăgirea ei. Prin ascultare activă și afirmarea sentimentelor interlocutorului, securitatea poate reduce tensiunea și poate stabili o legătură de încredere. De exemplu: ***"Înțeleg de ce te simți așa. Este frustrant să nu poți vizita un apropiat. Haide să discutăm despre asta într-un loc mai liniștit."***

Redirecționarea într-un spațiu liniștit: Ducerea vizitatoarei într-un spațiu separat și liniștit este o tehnică eficientă de a reduce stimulii exteriori și de a oferi un mediu propice pentru discuții. Acest lucru permite persoanei agitate să se simtă mai puțin asediată și poate ajuta la diminuarea sentimentului că este în centrul atenției.

Aceste tehnici, aplicate cu tact și empatie, pot ajuta la transformarea unei situații potențial explozive într-o discuție constructivă și calmă.

ZONELE SENSIBILE DIN PUNCT DE VEDERE AL SECURITĂȚII
ÎN UNITĂȚILE SANITARE

Practicienii în securitate, fac o distincție clară între zonele cu risc mai mare, deseori considerate zone cu probleme de securitate, și zonele cu preocupări speciale de securitate.

Toate unitățile sanitare trebuie să identifice riscurile de securitate din mediile lor respective care necesită protecție sporită sau măsuri speciale de siguranță.

Este responsabilitatea organizației de sănătate să decidă, printr-un proces de analiză a riscurilor de securitate, care zone prezintă un risc excepțional, făcându-le zone cu probleme de securitate sau zone cu risc mai scăzut dar de interes deosebit de asigurare a securității.

Pentru asigurarea securității unităților sanitare, este util să privim zonele de risc ridicat în două categorii.

Prima categorie implică vulnerabilitatea față de persoane, cum ar fi în secția obstetrică ginecologie, compartimentul de psihiatrie, zonele de parcare îndepărtate, zona de îngrijire clinică a departamentului de urgență și unitatea de terapie intensivă. **A doua categorie implică activele.**

Zonele cu bunuri valoroase din cadrul majorității unităților sanitare includ farmacia, zonele în care se păstrează dosarele medicale protejate, camerele serverelor de tehnologie și servicii informatice, laboratoarele de cercetare și zonele de manipulare a numerarului/casieriei.

În aceste cazuri, riscul de pierdere potențială se învârte în jurul unui produs sau al unei funcții.

De exemplu, medicamentele din farmacie creează un risc mai mare de jaf armat, însă potențialul de pierdere în bani pentru unitatea sanitară este destul de scăzut.

O definiție clară și precisă pentru ceea ce reprezintă o zonă de risc ridicat față de o zonă sensibilă din punct de vedere al securității nu a fost niciodată emisă.

În această prezentare, termenii vor fi folosiți în mod interschimbabil și definiți după cum urmează: o locație a cărei funcție sau activitate prezintă un mediu în care există un potențial semnificativ de rănire, răpire sau pierdere de securitate, care ar avea cel mai probabil un impact negativ grav asupra capacității organizației de a oferi îngrijiri de înaltă calitate pacienților.

Acest lucru se bazează adesea pe potențialul de violență sau de utilizare a armelor, în special împotriva populațiilor vulnerabile, cum ar fi persoanele în vârstă, copiii, precum și pe disponibilitatea drogurilor sau a zonelor de manipulare a numerarului.

ZONELE SENSIBILE DIN PUNCT DE VEDERE AL SECURITĂȚII

GHID GENERAL PENTRU UNITĂȚILE SANITARE

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid specific pentru industria de securitate pentru a ghida unitățile sanitare în identificarea și protejarea zonelor sensibile din punct de vedere al securității.

Declarație

Unitățile sanitare vor identifica zonele sensibile din punct de vedere al securității în timpul evaluărilor de risc la securitate și vor dezvolta măsuri rezonabile pentru a minimiza vulnerabilitățile și a atenua riscul.

Intenție

a. Zonele sensibile din punct de vedere al securității ar trebui identificate în timpul evaluării riscurilor și pot include:
    1. Zonele care adăpostesc populații cu risc, materiale controlate și periculoase sau echipamente și informații sensibile.
    2. Operațiuni cu un potențial semnificativ de vătămare, răpire sau pierdere.

b. Managerul zonelor sensibile identificate din punct de vedere al securității ar trebui să participe la eforturile de atenuare, iar planificarea ar trebui să includă securitatea, clinicienii și personalul auxiliar.

c. Unitatea sanitară ar trebui să dezvolte un plan pentru fiecare zonă sensibilă din punct de vedere al securității. Acolo unde este cazul, planul de securitate ar trebui să includă următoarele:
    1. Identificarea riscurilor specifice zonei.
    2. Plan de control al accesului de intrare și ieșire din zonă pentru vizitatori, pacienți, personal și alții.
    3. Tehnologia de securitate; aceasta poate include supraveghere video, monitorizare prin alarmă, sisteme de încuietori sau alte măsuri de securitate.
    4. Ar trebui dezvoltare, proceduri de întreținere preventivă pentru reducerea potențialului de eșec al sistemului de securitate, incluzând proceduri de testare regulată și continuă.
    5. Formare în securitate pentru membrii personalului și, după caz, pentru pacienți și familiile acestora.
    6. Realizarea unui plan de răspuns care stabilește, clar, rolurile și responsabilitățile pentru securitate, clinicieni și personalul auxiliar.
    7. Un proces de revizuire și acțiune corectivă a activităților și evenimentelor de securitate.

SECURITATEA UNITĂȚII DE PRIMIRI URGENȚE

Securitatea în unitățile de primiri urgențe este o provocare. Au existat numeroase acte violente comise în unitățile de primiri urgențe din România și din toată lumea, existând, chiar și cazuri în care au fost implicați atacatori înarmați.

De asemenea, au fost pacienți și/sau aparținători care i-au atacat pe doctori sau asistente medicale.

Aceste acte violente sunt devastatoare pentru personalul medical și ceilalți pacienți și nicio unitate sanitară nu este imună la acest fenomen dar, cu toate acestea, ele primesc doar atenție mediatică pe termen scurt. Violența în unitățile de primiri urgențe este ceva ce îngrijorează managementul unităților sanitare iar noi, ne-am propus să ajutăm în prevenirea și combaterea acestui fenomen.

În mod trist, cele mai frecvente acte de violență provin chiar de la pacienți.

Violența generată de pacienți apare în orice tip de sunitate de urgență, indiferent de mărime sau locație.

Un număr mare de cadre medicale au fost victime ale violenței fizice sau abuzului verbal din partea pacienților. Aceștia lovesc, scuipă, mușcă și zgârie personalul medical. De asemenea, folosesc un limbaj abuziv. Această violență poate duce la teamă în rândul personalului medical și provocări în recrutarea acestuia.

Secțiile de urgență vor avea întotdeauna caracteristici care cresc probabilitatea unui comportament perturbator. Factorii psihici și fizici extremi, manifestările psihiatrice acute, abuzul de droguri și alcool de către pacienți și vizitatori, amestecul de pacienți și personal nemedical contribuie la un mediu cu risc foarte ridicat.

Când se adaugă membrii bandelor rivale care apar cu arme, timpii lungi de așteptare din cauza aglomerării continue și amenințările zilnice de a avea grijă de victimele violenței domestice, secțiile de urgență sunt fără îndoială cele mai volatile zone din unitățile medicale.

Episoadele violente provoacă teamă personalului medical iar unele incidente de violență nu sunt raportate din teama de represalii din partea agresorilor.

Costurile emoționale, sociale și financiare ale violenței în unitățile de primiri urgențe sunt incalculabile.

Reducerea numărului de evenimente violente și minimizarea efectelor pe termen lung ale celor care au loc sunt priorități majore.

Comportamentul perturbator poate fi prevăzut și gestionat pentru a reduce la minimum riscurile și a asigura siguranța tuturor celor implicați.

Medicii și asistentele care lucrează în unitățile de primiri urgențe cer și au nevoie o mai bună protecție din partea unităților sanitare.

Comportamentul agresiv și violent în unitățile sanitare poate fi prevenit și gestionat printr-o serie de măsuri, cum ar fi politici clare, securitate fizică îmbunătățită, instruirea personalului, identificarea pacienților cu risc crescut și folosirea restricțiilor atunci când este necesar, pentru a asigura siguranța tuturor.

"Situația din unitățile de primiri urgențe din unele din spitalele noastre este extrem de îngrijorătoare. Indivizii care manifestă intenții agresive nu sunt monitorizați sau reținuți în mod corespunzător și nu există măsuri de securitate eficiente.

Această lipsă de acțiune preventivă pare chiar mai irațională decât comportamentul violent al acestor indivizi."

Dr. Robert Ieu

SECURITATEA UNITĂȚII DE PRIMIRI URGENȚE - GHID GENERAL

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid general de securitate pentru unitățile sanitare care oferă servicii de îngrijire de urgență.

Declarație

Unitățile sanitare care oferă asistență medicală de urgență au nevoi speciale de securitate și ar trebui să aibă un plan de securitate specific pentru acest departament.

Intenție

A. Planul ar trebui să se bazeze pe riscurile identificate pentru unitatea de primiri urgențe, inclusiv pe numărul și tipurile de pacienți tratați, tipurile și istoricul incidentelor și datele demografice ale comunității.

B. Managerul de securitate ar trebui să fie implicat în fazele de planificare, de construcție și/sau de renovare a unității de primiri urgențe, ca resursă în ceea ce privește aspectele legate de proiectarea de securitate.

   1. Sala de așteptare a unității de primiri urgențe ar trebui să fie separată de zona de tratament și să fie autonomă pentru a include acces independent la toalete.
   2. Ar trebui să existe controale de acces pentru a controla și a limita accesul vizitatorilor din unitatea de primiri urgențe în zona de tratament și în alte zone ale unității sanitare.
   3. Ar trebui să fie disponibilă o cameră sau o zonă în cadrul unității de primiri urgențe, separată de ceilalți pacienți, pentru tratamentul pacienților cu probleme de sănătate comportamentală/mentală sau a altor pacienți cu risc ridicat. Această cameră/zonă ar trebui să includă vizibilitatea de către personal și îndepărtarea sau asigurarea obiectelor care ar putea fi folosite de pacient pentru a se răni pe sine sau pe alții.
   4. Intrarea ambulanței ar trebui să fie separată de intrarea de urgență și de sala de așteptare.

C. Personalul de securitate oferă servicii de sprijin în unității de primiri urgențe. Aceste servicii sunt furnizate la cererea și sub conducerea și supravegherea personalului clinic, cu excepția cazului în care circumstanțele necesită o acțiune imediată pentru a preveni rănirea sau distrugerea bunurilor.

D. Trebuie să existe echipamente și sisteme de securitate pentru a proteja personalul și pacienții. Acestea pot include controlul electronic al accesului, supravegherea video și alarmele de panică. Unitatea de primiri urgențe ar trebui să poată fi închisă rapid în caz de urgență. Ar trebui să se efectueze exerciții pentru a exersa procesul de închidere.

E. Ar trebui să existe măsuri fizice și proceduri pentru a descuraja fuga și/sau îndepărtarea pacienților care riscă să se rănească pe ei înșiși, pe alții sau să fie răniți.

F. Personalul unității de primiri urgențe (inclusiv personalul de securitate) ar trebui să beneficieze de o formare continuă în domeniul violenței la locul de muncă, al gestionării pacienților agresivi/violenți pentru a recunoaște, evita, dezamorsa și răspunde la situații potențial violente.

G. Ar trebui să se organizeze întâlniri periodice, cel puțin o dată pe an, cu personalul multidisciplinar pentru a revizui protocoalele de securitate și pentru a rezolva problemele de securitate în cadrul unității de primiri urgențe.

H. Ar trebui stabilite politici, proceduri și programe de formare pentru rolul securității în gestionarea pacienților cu risc ridicat, inclusiv supravegherea pacienților, reținerile, percheziții și aplicarea de mijloace de imobilizare a pacienților.

PARCĂRILE UNITĂȚILOR SANITARE ȘI
MEDIUL EXTERN

Zonele de parcare ale unităților sanitare, fie că sunt suprafețe deschise sau structuri pe mai multe niveluri în cazul marilor spitale, de exemplu, pot fi locuri periculoase unde pot avea loc diferite activități infracționale și/sau accidente.

Cererea de parcări, în toate unitățile sanitare, a crescut semnificativ, în mare parte datorită extinderii serviciilor ambulatorii.

Multe dintre instrumentele folosite anterior pentru a estima nevoile de parcare sunt acum depășite. Deși parcarea a fost întotdeauna o preocupare majoră pentru unitățile sanitare, adesea nu se acordă atenția necesară planificării și securității. În România, nu avem cunoștiință despre vre-un sondaj pe tema locurilor de parcare în unitățile sanitare,dar sondaje realizate în alte țări arată că majoritatea spitalelor, de exemplu, consideră că nu au suficiente locuri de parcare.

Fiecare unitate sanitară are propriile caracteristici care influențează nevoile de parcare, controlul parcării fiind o activitate esențială pentru facilitățile medicale, uneori fiind responsabilitatea securității, alteori fiind atribuită altor departamente.

Necesitatea securității în parcările unităților sanitare

- **Furtul sau deteriorarea autovehiculelor.** Datorită naturii aglomerate a acestor parcări și a frecventei mari de utilizare, ele devin ținte pentru hoți sau vandali.
- **Amenințări la adresa integrității fizice.** Indivizii cu intenții malefice pot folosi parcările ca loc de așteptare sau de abordare a potențialelor victime.
- **Accidente.** Aglomerația și posibilele emoții intense ale celor care vizitează unitatea sanitară pot crește riscul de accidente auto sau de coliziuni.
- **Traversarea nesigură.** Pacienții, în special cei cu mobilitate redusă sau cu afecțiuni acute, pot întâmpina dificultăți în traversarea parcării, ceea ce crește riscul de accidente.

Strategii de asigurare a securității

Asigurarea securității în parcările unităților sanitare necesită o abordare complexă, care să includă atât măsuri preventive, cât și reactive:

- **Iluminat adecvat.** O lumină suficient de puternică poate descuraja acțiunile infractorilor și poate reduce riscul de accidente.
- **Camere de supraveghere.** Acestea pot fi deterrente eficiente pentru activitățile ilegale și pot oferi dovezi valoroase în cazul unor incidente.
- **Patrulare regulată.** Securitatea fizică, prin patrulele efectuate de personal de specialitate, este esențială pentru detectarea rapidă a oricăror probleme.
- **Semnalizare clară și vizibilă.** Indicatoarele clare pot preveni accidentele și pot ghida utilizatorii spre zonele sigure de parcare sau de traversare.
- **Bariere de acces și control.** Limitarea accesului doar la persoanele autorizate poate reduce semnificativ numărul de incidente.

Concluzie:

Securitatea parcărilor unităților sanitare este esențială nu doar pentru protejarea autovehiculelor, ci și pentru asigurarea unui mediu sigur și protejat pentru pacienți și angajați.

Într-o lume în care riscurile de securitate sunt în continuă evoluție, este imperativ ca unitățile sanitare să-și revizuiască constant și să-și îmbunătățească măsurile de securitate pentru a proteja pe toți cei care apelează la serviciile lor.

IAHSS (International Association for Healthcare Security & Safety) a elaborat un ghid general de securitate pentru parcările unităților sanitare. (EXTRAS)

Declarație

Unitățile sanitare vor încorpora principii generale de protecție în parcările lor pentru a menține o percepție pozitivă a siguranței personale a angajaților, vizitatorilor și pacienților și pentru a asigura un nivel rezonabil de securitate pentru toți cei care fac parte din acestea.

Intenție

A. Parcarea angajaților, inclusiv a personalului după orele de program, trebuie să fie separată de parcarea vizitatorilor. Vehiculele angajaților ar trebui să fie ușor de identificat prin utilizarea unui plan definit de management a parcării. Ar trebui să se prevadă parcări suplimentare pentru cei care lucrează în afara orelor tradiționale.

B. Ar trebui să se desemneze o parcare practică pentru pacienții și vizitatorii din departamentul de urgență.

C. Iluminatul oferă un mijloc de a menține, în timpul orelor de întuneric, un grad de protecție apropiat de cel menținut în timpul zilei. Pentru a fi eficient, iluminatul de protecție ar trebui să acționeze ca un factor de descurajare și să facă posibilă recunoașterea efectivă a persoanelor și activităților.

D. Barierele fizice de protecție pot contribui la restricționarea sau canalizarea accesului. Barierele fizice de protecție ar trebui să fie amplasate pe întreg amplasamentul pentru a reduce la minimum probabilitatea accidentării de către vehicule a pietonilor, a distrugerii echipamentelor și structurilor sensibile și pentru a nu obstrucționa vederea sau, a nu împiedica circulația vehiculelor. Barierele fizice pot fi completate cu senzori de mișcare și supraveghere video. Ar trebui puse în aplicare modificarea formelor de relief, integrarea elementelor decorative, a jardinierelor supraînălțate, a vegetației, a schimbărilor de înălțime a zonelor pavate, a gardurilor, a unei game largi de funcții stradale, a elementelor de amplasare și a facilităților ("bolarzi", bănci, stâlpi de iluminat, chioșcuri etc.). Ar trebui menținute linii de vizibilitate deschise pentru a reduce la minimum potențialele locuri de ascundere ("unghiuri moarte")

E. Modelele de trafic, capacitățile rețelei rutiere și capacitatea vehiculelor ar trebui analizate periodic. Obstacolele de trafic ar trebui să fie poziționate în apropierea punctelor de intrare pentru a încetini traficul și pentru a compensa intrările de vehicule din direcția de apropiere a unui vehicul pentru a forța o reducere a vitezei. Numărul de drumuri de acces și de intrări la un obiectiv ar trebui să fie redus la minimum (unele intrări pot fi închise și securizate în afara perioadelor de vârf). Intrările desemnate pentru vehiculele de serviciu și de livrare ar trebui să fie proiectate departe de clădirile cu risc ridicat. Vehiculele de urgență ar trebui să aibă acces liber la facilitate.

F. Accesul pietonilor la intrările publice nu ar trebui să fie împiedicat de accesul vehiculelor sau perturbat de-a lungul trotuarelor sau al altor coridoare de mers pe jos definite în zonele de parcare.

G. Amplasarea și utilizarea supravegherii video în zonele de parcare ar trebui să se bazeze pe o evaluare a riscului de securitate. Ar trebui să se ia în considerare următoarele:
1) punctele de intrare în parcări
2) punctele de control al vehiculelor
3) Dispozitivele de comunicare în caz de urgență amplasate în zonele de parcare
Ar trebui să se selecteze cu atenție echipamentul de supraveghere video și obiectivele adecvate care vor oferi rezultatele imaginii dorite și să se ia în considerare iluminatul, atât cel natural, cât și cel artificial, astfel încât să nu interfereze cu acoperirea sau vizualizarea camerei.

H. Dispozitivele de comunicare de urgență ("HELP") pot contribui la siguranța și securitatea parcărilor. Ar trebui să se ia în considerare să se acorde atenție amplasării strategice a dispozitivelor de comunicare în caz de urgență care sunt foarte vizibile de-a lungul aleilor pietonale și zonele de parcare.

I. Semnalizarea ar trebui să fie utilizată pentru a asigura conștientizarea securității în zonele de parcare, servind în același timp și ca mijloc de descurajare psihologică pentru infracțiuni și alte comportamente negative.

CAPITOLUL 9

PREGĂTIREA PENTRU SITUAȚII DE URGENȚĂ

Acest capitol prezintă orientările de bază privind securitatea în sectorul medical în ceea ce privește gestionarea situațiilor de urgență în domeniul sănătății.

PREGĂTIREA PENTRU SITUAȚIILE DE URGENȚĂ ÎN UNITĂȚILE SANITARE

PRIORITATE ȘI NECESITATE

Pregătirea pentru situații de urgență în unitățile sanitare este nu doar o responsabilitate, ci și o necesitate imperativă în lumea în care trăim.

Cu o gamă largă de riscuri posibile, de la acte de terorism până la dezastre naturale, planificarea și pregătirea adecvată pot face diferența între viață și moarte. Nu numai că pot salva viețile pacienților, dar pot proteja personalul, pot conserva resursele și pot menține integritatea sistemului de sănătate în ansamblu.

Dezastrele, fie ele naturale sau provocate de om, au un impact imediat și adesea devastator asupra infrastructurii medicale. Ele pot suprasolicita spitalele, de exemplu, pot duce la întreruperi ale furnizării de energie electrică și apă, și pot izola comunități întregi, făcând dificil accesul la asistență medicală.

În aceste momente, devine vital să avem un plan de acțiune bine gândit, testat și implementat pentru a menține funcționalitatea sistemului de sănătate și pentru a oferi asistență celor afectați.

Liderii din domeniul sănătății trebuie să ia în considerare mai multe aspecte atunci când concep un plan de pregătire pentru situații de urgență.

În primul rând, trebuie să fie efectuată o evaluare a riscului, pentru a înțelege tipurile de amenințări la care unitatea sanitară ar putea fi expusă. O astfel de evaluare ar trebui să includă factori precum localizarea geografică, proximitatea față de zonele cu risc ridicat de terorism sau dezastre naturale, și resursele disponibile în comunitate.

În al doilea rând, trebuie create protocoale clare de acțiune, care să fie cunoscute și înțelese de tot personalul. Acestea ar trebui să cuprindă proceduri pentru evacuare, triaj, comunicare inter-departamentală și externă, și alocarea resurselor în caz de urgență. Toate aceste protocoale ar trebui să fie adaptabile, pentru a putea face față unei varietăți de scenarii de urgență.

În al treilea rând, exerciții de simulare și antrenamente regulate sunt esențiale pentru a evalua eficacitatea planurilor și pentru a identifica punctele slabe. Aceste exerciții ar trebui să fie cât mai realiste posibil și să includă nu doar personalul medical, ci și alte entități cum ar fi forțele de ordine, pompierii și agențiile guvernamentale responsabile de gestionarea situațiilor de urgență.

În al patrulea rând, informarea și educarea publicului joacă un rol crucial. Pacienții și comunitatea în general ar trebui să fie conștienți de ce se întâmplă în caz de dezastre și cum să acționeze pentru a-și salva viața și a ajuta alții.

În cele din urmă, planificarea pentru situații de urgență trebuie să fie o componentă integrată în cultura și valorile organizației. Acest lucru nu numai că va ajuta la alocarea eficientă a resurselor, dar va și crește nivelul de încredere între comunitate și unitățile de sănătate. În acest mod, pregătirea pentru situații de urgență devine nu doar un plan de acțiune, ci parte din identitatea și misiunea organizației.

În concluzie, pregătirea pentru situații de urgență în unitățile sanitare nu este doar o necesitate, ci și o responsabilitate.

Este responsabilitatea managementului față de pacienți, față de personalul medical și față de societate în ansamblu să se asigure că sunt pregătiți să răspundă eficient și prompt în fața oricăror provocări.

IAHSS (International Association for Healthcare Security & Safety) a elaborat o serie de orientări de bază privind securitatea în sectorul medical în ceea ce privește gestionarea situațiilor de urgență în domeniul sănătății.

Declarație

Unitățile sanitare vor elabora și menține un program de gestionare a situațiilor de urgență pentru a identifica și aborda amenințările/pericolele/urgențele care pot avea un impact asupra unității și a operațiunilor sale.

Intenție

A. Trebuie desemnată o echipă multidisciplinară pentru a dezvolta, menține și aproba programul de gestionare a situațiilor de urgență.

   Echipa ar trebui să aibă sprijinul expres al managerului unității medicale, împreună cu autoritatea pentru program.

B. Securitatea ar trebui să aibă un rol clar definit în programul de gestionare a situațiilor de urgență al unității sanitare.

C. Programul de gestionare a situațiilor de urgență ar trebui să se bazeze pe cele patru faze de atenuare, pregătire, răspuns și recuperare.

D. Unitatea sanitară ar trebui să efectueze o analiză cuprinzătoare a vulnerabilității pericolelor/riscurilor pentru a identifica și prioritiza amenințările/pericolele/urgențele care pot avea un impact asupra operațiunilor sale. Această analiză ar trebui să fie revizuită anual și ori de câte ori apare o nouă amenințare/pericol/urgență.

E. Ar trebui să se elaboreze planuri multidisciplinare de răspuns în caz de urgență pentru a aborda potențialele amenințări identificate de unitatea sanitară.

F. Planurile de răspuns în caz de urgență ar trebui să aibă un sistem de comandă a incidentelor (SCI) pentru toate riscurile. Planurile de răspuns în caz de urgență ar trebui să abordeze nu numai răspunsul imediat și pe termen scurt al unității sanitare, ci și posibilitatea unor operațiuni de urgență care să dureze zile, săptămâni sau chiar mai mult.

G. Personalul unității sanitare ar trebui să primească educație și formare în domeniul managementului situațiilor de urgență în funcție de rolul cel mai probabil pe care îl va avea în răspunsul la eveniment.

H. Planurile de intervenție în caz de urgență ar trebui să fie exersate atât în scopul formării, astfel încât personalul să își înțeleagă rolurile și responsabilitățile și să se simtă confortabil în aceste roluri, cât și pentru a identifica și documenta punctele tari și slabe ale planurilor, precum și domeniile care trebuie îmbunătățite.

I. Planurile de urgență ar trebui să includă implicarea comunității, alte unități sanitare, echipele de intervenție în caz de urgență și agențiile guvernamentale.

J. Planurile de urgență ar trebui să includă prevederi pentru îngrijirea și bunăstarea personalului unității sanitare și a familiilor acestora.

PROGRAMUL DE GESTIONARE A SITUAȚIILOR DE URGENȚĂ PENTRU SPITALUL "MARIA" (EXEMPLU)

Declarație

Spitalul "Maria" se angajează să dezvolte și să mențină un program de gestionare a situațiilor de urgență pentru a identifica și aborda amenințările, pericolele și urgențele care pot afecta unitatea și operațiunile sale.

Intenție

A. Echipa de management a situațiilor de urgență
Spitalul "Maria" va numi o echipă multidisciplinară responsabilă pentru dezvoltarea, menținerea și aprobarea programului de gestionare a situațiilor de urgență. Această echipă va fi formată din reprezentanți din diferite departamente, inclusiv personal medical, securitate, managementul riscului și comunicare. Echipa va fi condusă de managerul spitalului și va avea sprijinul autorităților necesare pentru implementarea programului.

B. Rolul securității
Departamentul de securitate va juca un rol clar definit în programul de gestionare a situațiilor de urgență, asigurând securitatea pacienților, personalului și a bunurilor spitalului în timpul situațiilor de urgență.

C. Fazele de gestionare
Programul va fi structurat în jurul celor patru faze ale gestionării situațiilor de urgență: atenuare, pregătire, răspuns și recuperare.

D. Analiză a vulnerabilității și prioritizarea riscurilor
Spitalul "Maria" va efectua o analiză cuprinzătoare a vulnerabilității la pericole și riscuri pentru a identifica și prioritiza amenințările potențiale și urgențele care ar putea afecta operațiunile spitalului. Această analiză va fi revizuită anual și ori de câte ori apare o nouă amenințare sau pericol.

E. Planuri de răspuns multidisciplinare
Planuri de răspuns în caz de urgență vor fi elaborate pentru a aborda amenințările identificate. Aceste planuri vor implica departamente și specialiști relevanți pentru fiecare scenariu de urgență.

F. Sistem de comandă a incidentelor (SCI)
Toate planurile de răspuns în caz de urgență vor include un Sistem de Comandă a Incidentelor (SCI) pentru coordonarea eficientă a eforturilor în timpul situațiilor de urgență, inclusiv situații care pot dura zile, săptămâni sau mai mult.

G. Educație și formare
Personalul spitalului va primi educație și formare în domeniul gestionării situațiilor de urgență în funcție de rolul lor previzibil în răspunsul la eveniment.

H. Exerciții și testări
Planurile de răspuns în caz de urgență vor fi exersate și testate regulat pentru a asigura înțelegerea și eficacitatea lor. Aceste exerciții vor ajuta la identificarea punctelor tari și slabe ale planurilor și la îmbunătățirea acestora.

I. Colaborare cu comunitatea și agențiile guvernamentale
Planurile de urgență vor include colaborarea cu comunitatea locală, alte unități medicale, echipele de intervenție în caz de urgență și agențiile guvernamentale pentru a asigura un răspuns coordonat în situații de urgență.

J. Îngrijirea și bunăstarea personalului și a familiilor
Planurile de urgență vor include prevederi pentru îngrijirea și susținerea personalului spitalului și a familiilor acestora în timpul și după situațiile de urgență.

Acest **Program de Gestionare a Situațiilor de Urgență** va fi periodic revizuit și actualizat pentru a se adapta la noile amenințări și schimbări în mediul de securitate, asigurând astfel siguranța pacienților, a personalului și a întregii comunități.

CAPITOLUL 10

SECURITATEA CIBERNETICĂ MANAGEMENTUL SECURITĂȚII INFORMAȚIEI PROTECȚIA DATELOR CU CARACTER PERSONAL

Acest capitol prezintă amenințările cibernetice la adresa unităților sanitare și importanța securității informațiilor medicale.

Acoperă bune practici pentru protejarea rețelelor, sistemelor și datelor pacienților de atacuri ransomware, furt de identitate și încălcări ale confidențialității.

Explică regulamentele privind protecția datelor și cele mai bune metode de conformare, inclusiv autentificarea utilizatorilor, criptarea, copii de rezervă și conștientizarea personalului. Subliniază nevoia unei abordări cuprinzătoare în managementul securității informațiilor.

SECURITATEA CIBERNETICĂ ÎN UNITĂȚILE SANITARE

Securitatea cibernetică în unitățile sanitare reprezintă o provocare dublă: pe de o parte, mediul în care activează se schimbă rapid, devenind tot mai interconectat atât în interiorul sistemului de sănătate, cât și cu alte sectoare.

Această interconectare sporește suprafața de atac, crescând exponențial riscul de securitate.

Pe de altă parte, capacitatea de răspuns a acestor organizații este limitată de sistemele IT vechi și complexe, vulnerabile la atacuri cibernetice, și de o lipsă a culturii, competențelor și a capacităților tehnice în domeniul securității cibernetice.

Astăzi, majoritatea activităților și proceselor din cadrul unităților sanitare sunt susținute de tehnologiile informației și comunicațiilor (TIC) și sunt bazate pe date.

Prin urmare, datele și informațiile au devenit active critice în cadrul organizației, necesitând un nivel ridicat de protecție atât pentru confidențialitate, cât și pentru securitate.

Dificultățile de protecție cresc în condițiile unui număr mare de sisteme și dispozitive interconectate și a nevoii de a schimba date în afara granițelor organizaționale, la nivel național și internațional.

Un alt aspect de subliniat este faptul că, spre deosebire de informațiile financiare, datele de sănătate nu pot fi schimbate odată ce au fost furate.

Acest lucru le face mult mai valoroase pe piața neagră, fiind considerate de până la cincizeci de ori mai valoroase decât informațiile financiare.

Drept urmare, încălcările de date devin din ce în ce mai frecvente în sectorul sănătății.

Amenințările nu se limitează doar la acțiuni cu intenție rea; erorile umane și defecțiunile sistemelor, precum și eșecurile terților, au un rol important.

Capacitatea de răspuns la aceste provocări este adesea compromisă de lipsa de pregătire și conștientizare în rândul profesioniștilor cu privire la riscurile și problemele de securitate cibernetică.

Aceste atacuri, pe lângă pierderile financiare și prejudiciul de reputație, diminuează încrederea pacienților în modul în care informațiile lor de sănătate sunt tratate și stocate în infrastructura digitală, ceea ce reprezintă o provocare pentru eforturile de inovare digitală ale organizației.

Pentru a aborda aceste provocări, este necesar un răspuns complex.

Acesta începe cu adoptarea unor strategii care să identifice și să trateze vulnerabilitățile existente, să pregătească și să implice forța de muncă și să informeze politicile de achiziție tehnologică.

Oamenii, procesele și tehnologia reprezintă cele trei piloni ai unui sistem de sănătate mai rezistent și mai sigur, cu un nivel ridicat de încredere din partea utilizatorilor în tehnologiile digitale.

Este esențială formarea și sensibilizarea personalului, îmbunătățirea sistemelor tehnice și crearea unei culturi organizaționale care pune accentul pe securitatea cibernetică pentru a proteja eficient informațiile și datele pacienților.

AMENINȚĂRILE CIBERNETICE ÎN UNITĂȚILE SANITARE

Unitățile sanitare sunt o țintă a amenințărilor cibernetice din cauza datelor sensibile pe care le dețin, cum ar fi informații despre pacienți, istoric medical, date financiare și informații despre echipamente medicale.

Aceste atacuri pot avea un impact semnificativ asupra funcționării unității, putând duce la întreruperea serviciilor medicale, la pierderea datelor medicale și la costuri financiare semnificative.

Cele mai frecvente tipuri de amenințări cibernetice în unitățile sanitare:

- **Malware** - viruși, viermi și troieni care pot perturba sistemele informatice și fura date.
- **Ransomware:** Unul dintre cele mai răspândite tipuri de atacuri, ransomware-ul criptează datele și cere o răscumpărare pentru decriptarea lor. Într-o unitate sanitară, acest tip de atac poate paraliza întregul sistem, afectând îngrijirea pacientului.
- **Phishing:** Acest tip de atac presupune trimiterea de e-mailuri false care încearcă să păcălească angajații să dezvăluie informații confidențiale, cum ar fi parolele.
- **Atacuri DDoS:** Aceste atacuri încarcă serverele cu trafic fals, făcând imposibilă utilizarea rețelei. Astfel de atacuri pot împiedica accesul la informațiile critice ale pacienților.
- **Încălcarea datelor:** Este vorba de accesul neautorizat la bazele de date ale unității sanitare, ce poate duce la furtul de informații sensibile despre pacienți și personal.
- **Atacuri interne:** Provocate, uneori, de angajați nemulțumiți sau neinstruiți corespunzător, aceste atacuri pot fi devastatoare.
- **Dispozitive neactualizate:** Echipamentele medicale vechi sau neactualizate pot fi vulnerabile la atacuri, permițând hackerilor să preia controlul dispozitivelor.

Atacurile cibernetice - consecințe:

- **Întreruperea serviciilor medicale:** Un atac cibernetic poate duce la întreruperea accesului la sisteme informatice vitale, cum ar fi sistemele de înregistrare a pacienților, sistemele de imagistică medicală sau sistemele de monitorizare a pacienților.
- **Distrugerea datelor:** Un atac cibernetic poate duce la distrugerea datelor, ceea ce poate afecta capacitatea unității sanitare de a oferi îngrijiri medicale.
- **Furtul de date:** Acest lucru poate fi folosit pentru a comite fraude sau pentru a ține șantaj.
- **Pierderea datelor medicale:** Acest lucru poate avea un impact negativ asupra confidențialității pacienților și poate duce la erori în diagnostic și tratament.
- **Costuri financiare semnificative:** Un atac cibernetic poate duce la costuri financiare semnificative, inclusiv costuri de recuperare a datelor, costuri de reparare a sistemelo r informatice și costuri de despăgubire a pacienților.

Unitățile sanitare pot lua o serie de măsuri pentru a se proteja împotriva atacurilor cibernetice, inclusiv:

- ❑ Investirea în securitate cibernetică: Unitățile sanitare ar trebui să investească în soluții de securitate cibernetică de ultimă generație, cum ar fi firewall-uri, sisteme de detectare și răspuns la intruzii (IDS/IPS) și soluții de back-up și recuperare a datelor.
- ❑ Educarea angajaților cu privire la securitatea cibernetică: Angajații unităților sanitare ar trebui să fie instruiți cu privire la practicile de securitate cibernetică, cum ar fi utilizarea de parole puternice și evitarea deschiderii de e-mailuri sau fișiere suspecte.
- ❑ Implementarea de politici și proceduri de securitate cibernetică: Unitățile sanitare ar trebui să implementeze politici și proceduri de securitate cibernetică care să definească rolurile și responsabilitățile angajaților în ceea ce privește securitatea cibernetică.

RECOMANDĂRI PENTRU MANAGEMENT:

- **Creați un comitet de securitate cibernetică:** Un comitet de securitate cibernetică este responsabil pentru dezvoltarea și implementarea politicilor de securitate cibernetică.
- **Alocați un buget pentru securitatea cibernetică:** Securitatea cibernetică este o investiție importantă, iar managementul unităților sanitare trebuie să aloce un buget adecvat pentru a implementa măsuri de securitate cibernetică.
- **Testați periodic sistemele informatice:** Sistemele informatice trebuie testate periodic pentru a identifica vulnerabilitățile.
- **Monitorizați activitatea în rețea:** Sistemele de monitorizare a rețelei pot ajuta la detectarea activității suspecte.
- **Fiți pregătiți pentru un atac cibernetic:** Unitățile sanitare trebuie să aibă un plan de răspuns la un atac cibernetic.

IMPLEMENTAREA UNUI SISTEM DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ÎN UNITĂȚILE SANITARE

Protejarea datelor și informațiilor a devenit, astăzi, esențială pentru orice instituție, iar în sectorul sănătății, unde datele sunt atât de sensibile și critice, această protecție devine imperativă.

Autorii consideră că implementarea unui sistem de management al securității informației (SMSI) în unitățile sanitare reprezintă o prioritate majoră.

A. Contextul și importanța SMSI în unitățile sanitare:

Datele pacienților, cum ar fi istoricul medical, informațiile de contact, dar și informațiile financiare, sunt esențiale pentru furnizarea serviciilor medicale. Orice încălcare a acestor date nu doar că ar putea avea consecințe legale, dar ar putea eroda încrederea pacientului în unitatea sanitară și ar putea expune pacienții la riscuri de confidențialitate.

B. Pașii necesari implementării SMSI:

1. **Analiza de risc:** Înainte de a dezvolta și implementa un SMSI, este esențial să se efectueze o analiză cuprinzătoare a riscului pentru a identifica potențialele amenințări și vulnerabilități.
2. **Alegerea unui cadru de lucru:** Există mai multe cadre de lucru pentru SMSI, cel mai popular fiind ISO 27001. Acest standard internațional oferă linii directoare privind securitatea informațiilor într-un context general, care poate fi adaptat la specificul unităților sanitare.
3. **Formularea politicii de securitate:** Aceasta ar trebui să definească angajamentul organizației față de securitatea informațiilor, precum și responsabilitățile angajaților.
4. **Implementarea măsurilor de securitate:** Acestea pot varia de la soluții tehnice, cum ar fi firewalls sau criptarea datelor, la proceduri operaționale și formare pentru angajați.
5. **Audit și revizuire:** Odată ce SMSI este în vigoare, este crucial să se efectueze audituri regulate pentru a identifica eventualele puncte slabe și a asigura că sistemul funcționează eficient.

C. Beneficiile SMSI în unitățile sanitare:

1. **Confidențialitate:** Asigură că datele pacienților sunt accesate doar de persoanele autorizate.
2. **Integritate:** Datele sunt protejate împotriva modificărilor neautorizate.
3. **Disponibilitate:** Informațiile sunt accesibile atunci când sunt necesare, fără întreruperi neașteptate.
4. **Îmbunătățirea reputației:** Pacienții vor avea mai multă încredere în unitatea sanitară știind că datele lor sunt în siguranță.

D. Provocările implementării SMSI:

Ca orice sistem, și SMSI vine cu propriile sale provocări, inclusiv rezistența la schimbare din partea angajaților, costurile asociate cu implementarea și necesitatea formării continue.

CONCLUZIE:

În contextul actual, unde amenințările cibernetice sunt în creștere și legislația privind protecția datelor devine din ce în ce mai stringentă, implementarea unui SMSI în unitățile sanitare nu mai este o opțiune, ci o necesitate.

Cu planificare adecvată și angajament din partea conducerii și a angajaților, unitățile sanitare pot asigura protecția eficientă a datelor și pot furniza servicii de calitate pacienților lor fără teama de încălcări de securitate.

IMPACTUL REGULAMENTULUI GENERAL PRIVIND PROTECȚIA DATELOR (GDPR)

ASUPRA UNITĂȚILOR SANITARE

Regulamentul General privind Protecția Datelor (GDPR) a adus cu el schimbări semnificative în modul în care organizațiile din întreaga Uniune Europeană colectează, procesează și stocează datele cu caracter personal.

Pentru unitățile sanitare, aceste schimbări sunt de o importanță deosebită datorită naturii sensibile a informațiilor de sănătate.

Această prezentare abordează principalele impacturi ale GDPR asupra unităților sanitare.

Datele sensibile: Unitățile sanitare procesează unele dintre cele mai sensibile tipuri de date cu caracter personal: informații medicale. GDPR clasifică aceste date ca fiind "categorie specială de date", ceea ce înseamnă că sunt necesare condiții speciale pentru prelucrarea lor. Aceasta impune unităților sanitare să aibă un motiv juridic puternic pentru a procesa aceste date și, de obicei, să obțină consimțământul explicit al pacientului.

Drepturile persoanelor vizate: GDPR a consolidat drepturile individuale în ceea ce privește datele lor personale. Pacienții au dreptul de a accesa, corecta, șterge și portabilitatea datelor lor. Acest lucru înseamnă că spitalele și clinicile trebuie să aibă proceduri eficiente pentru a răspunde la aceste solicitări în termenul legal de 30 de zile.

Măsuri de securitate: Datorită naturii sensibile a datelor pe care le prelucrează, unitățile sanitare sunt obligate să implementeze măsuri tehnice și organizatorice adecvate pentru a proteja datele. Aceasta include criptarea datelor, asigurarea confidențialității și integrității datelor, precum și capacitatea de a restabili disponibilitatea datelor în cazul unui incident.

Notificarea încălcărilor de securitate: GDPR introduce o obligație pentru organizații, inclusiv unitățile sanitare, de a raporta orice încălcare de securitate care afectează datele cu caracter personal către autoritatea de supraveghere competentă în termen de 72 de ore. Aceasta este o cerință majoră, având în vedere potențialele riscuri la adresa reputației și sancțiunile semnificative ce pot fi aplicate în cazul nerespectării.

Rolul Responsabilului cu Protecția Datelor (DPO): Multe unități sanitare sunt obligate să numească un DPO. Această persoană are rolul de a monitoriza conformitatea cu GDPR, a oferi sfaturi în legătură cu evaluările impactului asupra protecției datelor și a acționa ca punct de contact pentru subiecții de date și autoritatea de supraveghere.

Parteneri și furnizori: Contractele cu furnizorii și partenerii care procesează date cu caracter personal în numele unităților sanitare trebuie revizuite. Aceasta pentru a se asigura că există garanții adecvate pentru protejarea datelor și că responsabilitățile sunt clar definite.

Consimțământul și transparența: GDPR subliniază importanța unui consimțământ liber și informat. Unitățile sanitare trebuie să se asigure că formularele lor de consimțământ sunt clare și că pacienții înțeleg ce se va întâmpla cu datele lor. Aceasta include furnizarea de informații detaliate într-o formă accesibilă și ușor de înțeles.

Formare și conștientizare: Este esențial ca tot personalul unităților sanitare să fie instruit și conștient de obligațiile lor în virtutea GDPR. Aceasta nu numai pentru a evita încălcările, ci și pentru a proteja pacienții și integritatea instituției.

GDPR reprezintă mai mult decât o simplă listă de cerințe pentru unitățile sanitare. Este un apel la acțiune pentru a trata cu cea mai mare seriozitate și respect datele sensibile ale pacienților.

PRELUCRAREA DATELOR CU CARACTER PERSONAL
ÎN CONTEXTUL RELAȚIILOR DE MUNCĂ ÎN UNITĂȚILE SANITARE

În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

A. **interesele legitime urmărite de angajator sunt temeinic justificate** şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

B. **angajatorul a realizat informarea** prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

C. **angajatorul a consultat sindicatul** sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

D. **alte forme şi modalităţi mai puţin intruzive** pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa;

E. **durata de stocare a datelor cu caracter personal** este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

*(**Art. 5 din LEGEA nr. 190 din 18 iulie 2018** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).*

Legislația din România privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor prevede obligativitatea ca ***"unităţile şi instituţiile de interes public (aici se încadrează şi unităţile sanitare) trebuie să prevadă sisteme de supraveghere video pe căile de acces, holuri şi alte zone cu risc ridicat"*** iar acest lucru este prevăzut în **"Raportul de evaluare şi tratare a riscurilor la securitatea fizică"** întocmit de un expert în evaluarea riscului la securitatea fizică.

ATENȚIE! Măsurile stabilite în "Raportul de evaluare şi tratare a riscurilor la securitatea fizică" sunt obligatorii pentru unitatea sanitară.

Pentru a înțelege mai bine cerințele celor cinci puncte prevăzute de lege, am utilizat exemple ipotetice referindune la un spital, pe care l-am denumit " Spitalul Maria".

A. Justificarea intereselor legitime ale angajatorului pentru Spitalul Maria

Spitalul Maria, aflat în centrul orașului, găzduiește zilnic sute de pacienți și are un număr semnificativ de angajați. Având în vedere amplasarea sa și fluxul mare de persoane, pot apărea riscuri specifice legate de securitatea fizică. Recent, un "Raport de evaluare și tratare a riscurilor la securitatea fizică" a fost realizat de un expert în evaluarea riscului. Acest raport a identificat zonele cu risc ridicat și a evidențiat nevoia de sisteme de supraveghere video pe căile de acces, holuri și în acele zone.

- **Conformitatea cu legislația:** Spitalul Maria are obligația legală de a implementa măsurile stabilite în "Raportul de evaluare și tratare a riscurilor la securitatea fizică". Astfel, pentru a se conforma legislației în vigoare, introducerea sistemelor de supraveghere video este o necesitate, iar interesul angajatorului se aliniază direct cu prevederile legale.
- **Siguranța personalului și a pacienților:** Respectând măsurile din raport, Spitalul Maria asigură un mediu de lucru și de îngrijire mai sigur pentru angajați și pacienți. Un sistem de supraveghere poate descuraja activitățile neautorizate și poate acționa ca măsură preventivă împotriva incidentelor de securitate.
- **Protecția activelor spitalului:** Monitorizarea zonelor cu risc ridicat, precum depozitele de echipamente sau farmacia spitalului, reduce posibilitatea furturilor sau a utilizării necorespunzătoare a resurselor.
- **Responsabilitatea față de comunitate:** Ca unitate sanitară majoră, Spitalul Maria are o responsabilitate față de comunitatea pe care o deservește. Asigurarea unui mediu securizat contribuie la încrederea comunității în serviciile spitalului și la buna funcționare a acestuia.

În concluzie, având în vedere obligația legală și responsabilitățile ce decurg din aceasta, introducerea unui sistem de monitorizare video la Spitalul Maria reprezintă un interes legitim al angajatorului. Aceasta nu doar că îndeplinește prevederile legale, dar se asigură că spitalul oferă un mediu de lucru și de îngrijire securizat pentru toți cei implicați.

B. Informarea prealabilă a angajaților Spitalului Maria

Pe baza "Raportului de evaluare și tratare a riscurilor la securitatea fizică", Spitalul Maria a decis să instaleze sisteme de supraveghere video pe căile de acces, holuri și în alte zone cu risc ridicat, conform prevederilor legale.

Pentru a respecta principiul informării prealabile, conducerea spitalului dorește să informeze angajații cu privire la această schimbare.

Strategia de informare:

- **Întrunire cu personalul:** Conducerea spitalului organizează o întâlnire generală cu toți angajații. În cadrul acesteia, managerul spitalului și managerul de securitate prezintă "Raportul de evaluare și tratare a riscurilor la securitatea fizică", explicând zonele cu risc și motivul instalării camerelor de supraveghere.
- **Distribuirea unui memorandum:** Fiecare angajat primește un memorandum scris, care detaliază scopul monitorizării, zonele care vor fi supravegheate, precum și drepturile pe care le au angajații în contextul prelucrării datelor cu caracter personal.
- **Training:** Un scurt training privind protecția datelor personale este organizat pentru a ajuta angajații să înțeleagă drepturile și responsabilitățile lor în contextul GDPR. Acesta se axează pe importanța securității, prelucrarea datelor în contextul supravegherii video și măsurile luate de spital pentru a proteja drepturile angajaților.
- **Panouri informative:** În zonele unde sunt amplasate camerele de supraveghere se montează panouri informative care anunță prezența acestora și scopul pentru care sunt folosite, conform prevederilor GDPR.
- **Linie deschisă pentru întrebări:** Spitalul pune la dispoziție o linie telefonică sau o adresă de e-mail dedicată unde angajații pot adresa întrebări sau își pot exprima preocupările legate de sistemul de supraveghere.

În concluzie, Spitalul Maria își asumă responsabilitatea de a informa în mod corespunzător și transparent angajații despre instalarea sistemului de supraveghere video, oferindu-le resurse și informații clare cu privire la drepturile lor și motivele pentru care această măsură este necesară.

C. Consultarea sindicatelor sau reprezentanților angajaților Spitalului Maria

În urma deciziei de a instala camere de supraveghere bazate pe "Raportul de evaluare și tratare a riscurilor la securitatea fizică", conducerea Spitalului Maria dorește să respecte toate prevederile legale, inclusiv consultarea sindicatelor sau, în lipsa acestora, a reprezentanților angajaților.

Procedura de consultare:

1. **Notificare prealabilă:** Conducerea spitalului trimite o notificare oficială către sindicatul angajaților sau către reprezentanții aleși, informându-i despre intenția de a instala camere de supraveghere și solicitând o întâlnire formală pentru consultări.
2. **Întâlnirea de consultare:** O sesiune specială de consultare este programată, la care participă reprezentanții conducerii spitalului, reprezentanții sindicatului sau ai angajaților și expertul în securitate care a realizat raportul.

   În cadrul acestei întâlniri:
   - ☐ Se prezintă detaliile din "Raportul de evaluare și tratare a riscurilor la securitatea fizică".
   - ☐ Se discută zonele propuse pentru supraveghere.
   - ☐ Se prezintă motivele pentru care aceste măsuri sunt considerate necesare.
   - ☐ Se ascultă feedback-ul și preocupările sindicatului sau ale reprezentanților angajaților și se răspunde la întrebări.
3. **Înregistrarea feedback-ului:** Toate sugestiile, preocupările și recomandările oferite de sindicat sau reprezentanții angajaților sunt înregistrate formal.

4. **Revizuirea planului inițial:** În funcție de feedback-ul primit, conducerea spitalului poate decide să modifice anumite aspecte ale planului de implementare a sistemului de supraveghere, pentru a se alinia mai bine la nevoile și preocupările angajaților.
5. **Comunicare finală:** După finalizarea consultărilor și ajustarea planului, dacă este cazul, conducerea spitalului trimite o comunicare finală către sindicat sau reprezentanți, prezentând deciziile luate și pașii următori.

În concluzie, Spitalul Maria dă dovadă de transparență și respect față de drepturile angajaților, implicând activ sindicatul sau reprezentanții în deciziile care îi afectează, în conformitate cu prevederile legale.

D. Căutarea alternativelor mai puțin intruzive pentru Spitalul Maria

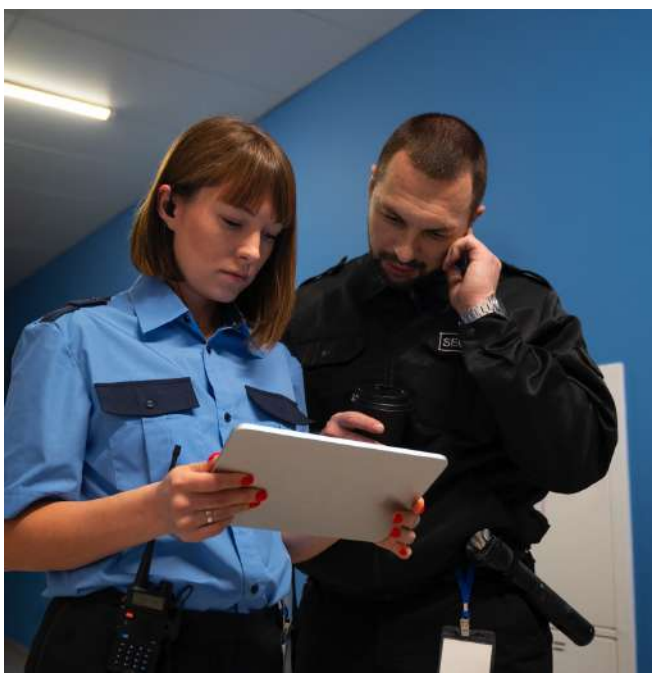
În urma analizei din "Raportul de evaluare și tratare a riscurilor la securitatea fizică", Spitalul Maria consideră instalarea camerelor de supraveghere în anumite zone critice.

Însă, pentru a respecta prevederile GDPR, conducerea spitalului dorește să analizeze și alternative mai puțin intruzive pentru securitate înainte de a lua o decizie definitivă privind supravegherea video.

Pasii urmați:

1. **Audit intern:** Conducerea spitalului solicită un audit intern pentru a identifica metode alternative de securitate care ar putea fi eficiente și mai puțin intruzive.
2. **Propuneri alternative:** După finalizarea auditului, sunt propuse următoarele soluții:
   - **Agenți de securitate:** Angajarea unui număr suplimentar de agenți de securitate pentru patrulare și supraveghere directă a zonelor cu risc ridicat.
   - **Acces cu cartelă:** Implementarea unui sistem de control al accesului prin cartele pentru anumite zone sensibile ale spitalului, limitând astfel accesul doar la personalul autorizat.
   - **Senzori de mișcare:** Instalarea de senzori de mișcare în anumite zone care pot alerta securitatea în cazul unei intrări neautorizate.
   - **Iluminat suplimentar:** Optimizarea iluminatului în zonele cu risc, descurajând astfel activitățile suspecte
3. **Evaluare eficiență:** Fiecare propunere este evaluată în funcție de costuri, fezabilitate și eficiența potențială în comparație cu supravegherea video.
4. **Decizia finală:** După analiza alternativelor, conducerea spitalului constată că:
   - Agenții de securitate sunt eficienți, dar costurile pe termen lung sunt semnificativ mai mari.
   - Sistemele de acces cu cartelă și senzorii de mișcare sunt utile, dar nu oferă aceeași acoperire comprehensivă ca și camerele de supraveghere.
   - Îmbunătățirea iluminatului este benefică, dar nu adresează direct toate riscurile identificate.
5. **Implementare mixtă:** În urma evaluării, Spitalul Maria decide să implementeze un sistem mixt: instalarea de camere de supraveghere în zonele cu risc ridicat, îmbunătățirea iluminatului în anumite zone și implementarea controlului accesului prin cartele pentru anumite secții.

În concluzie, Spitalul Maria demonstrează un angajament de a găsi soluții echilibrate, ținând cont atât de nevoia de securitate, cât și de dreptul la intimitate al angajaților și pacienților.



E. Durata de stocare a datelor pentru Spitalul Maria

Pentru a se alinia cu prevederile GDPR și cu legislația națională, Spitalul Maria analizează modul în care se stochează datele provenite din sistemele de supraveghere video și caută o metodologie care să se conformeze termenului de stocare permis.

Procedură de aplicare:

1. **Evaluarea nevoilor de stocare:** Departamentul IT al Spitalului Maria, în colaborare cu echipa de securitate, realizează o evaluare a nevoilor reale de stocare, ținând cont de zonele monitorizate și de evenimentele care ar putea necesita o revizuire a înregistrărilor video.
2. **Setarea automată a sistemelor:** Sistemul de supraveghere este configurat astfel încât să șteargă automat înregistrările care depășesc 30 de zile, asigurându-se astfel conformitatea cu prevederile legale.
3. **Excepții:** Pentru situații în care există motive temeinic justificate (de exemplu, investigarea unui incident de securitate sau o solicitare legală), anumite segmente din înregistrări pot fi păstrate peste perioada de 30 de zile. Aceste excepții sunt documentate corespunzător, menționând motivul păstrării și durata estimată de stocare.
4. **Accesul limitat:** Accesul la înregistrările video este strict limitat la personalul autorizat. Orice solicitare externă de acces la aceste înregistrări (de exemplu, de la forțele de ordine) este tratată cu mare atenție, și este furnizată numai în baza unei solicitări oficiale.
5. **Revizuire periodică:** Spitalul Maria efectuează o revizuire periodică a politicii de stocare a datelor pentru a se asigura că practicile rămân actuale și în conformitate cu legislația.
6. **Informarea angajaților:** Angajații sunt informați despre durata de stocare a datelor și despre drepturile lor în relație cu aceste înregistrări, inclusiv dreptul de acces și dreptul de a cere ștergerea înregistrărilor în anumite circumstanțe, în măsura în care acest lucru este permis de lege.

În concluzie, prin aceste măsuri, Spitalul Maria se asigură că respectă atât obligativitatea de a avea sisteme de supraveghere, cât și drepturile individuale ale persoanelor înregistrate, conform prevederilor GDPR.

Prelucrarea datelor cu caracter personal şi de categorii speciale de date cu caracter personal, în contextul îndeplinirii unei sarcini care serveşte unui interes public. În cazul în care prelucrarea datelor personale şi speciale este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public conform art. 6 alin. (1) lit. e) şi art. 9 lit. g) din Regulamentul general privind protecţia datelor se efectuează cu instituirea de către operator sau de către partea terţă a următoarelor garanţii:

a. **punerea în aplicare a măsurilor tehnice şi organizatorice** adecvate pentru respectarea principiilor enumerate la art. 5 din Regulamentul general privind protecţia datelor, în special a reducerii la minimum a datelor, respectiv a principiului integrităţii şi confidenţialităţii;
b. **numirea unui responsabil pentru protecţia datelor**, dacă aceasta este necesară în conformitate cu art. 10 din prezenta lege;
c. **stabilirea de termene de stocare** în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

(Art. 6 din LEGEA nr. 190 din 18 iulie 2018)

CONTRACT DE ÎMPUTERNICIT AL OPERATORULUI
(exemplu)

CONTRACT DE ÎMPUTERNICIT AL OPERATORULUI

ÎNTRE:

1. Spitalul "Maria", denumit în continuare **"Operatorul",** cu sediul în .... reprezentată de ..., în calitate de .... [Funcția Reprezentantului] și

2. "iQuality Services", denumită în continuare **"Persoana Împuternicită de Operator"**, cu sediul .... înregistrată la Registrul Comerțului sub nr. ..., reprezentată de ...., în calitate de [Funcția Reprezentantului];
în considerarea obligațiilor stabilite în Regulamentul (UE) 2016/679 (GDPR), părțile convin să încheie prezentul contract astfel:

PREAMBUL:

Operatorul intenționează să prelucreze date cu caracter personal prin intermediul unui sistem de supraveghere video, iar în acest sens, a solicitat Persoanei Împuternicite de Operator să instaleze și să asigure mentenanța sistemului de supraveghere video.

Art. 1: Obiectul Contractului

Persoana Împuternicită de Operator se angajează să prelucreze datele cu caracter personal în numele Operatorului, în conformitate cu prevederile prezentului contract și cu instrucțiunile Operatorului.

Art. 2: Instrucțiuni Documentate

Persoana Împuternicită de Operator va prelucra datele cu caracter personal exclusiv conform instrucțiunilor documentate ale Operatorului. Orice alte prelucrări neautorizate în mod explicit de Operator sunt interzise.

Art. 3: Confidențialitate

Persoana Împuternicită de Operator garantează confidențialitatea datelor cu caracter personal și asigură că persoanele autorizate să prelucreze datele au obligația de confidențialitate.

Art. 4: Securitatea Prelucrării

În conformitate cu Art. 32 din GDPR, Persoana Împuternicită de Operator va lua toate măsurile tehnice și organizatorice necesare pentru a asigura securitatea datelor.

Art. 5: Sub-împuterniciți

Fără a obține o autorizare prealabilă și scrisă de la Operator, Persoana Împuternicită de Operator nu va angaja niciun sub-împuternicit.

Art. 6: Drepturile Persoanelor Vizate

Persoana Împuternicită de Operator va asista Operatorul în asigurarea exercitării drepturilor persoanelor vizate, în conformitate cu Art. 28(3)(e) din GDPR.

Art. 7: Asistență

Persoana Împuternicită de Operator va oferi asistență Operatorului în îndeplinirea obligațiilor sale, ținând cont de natura prelucrării și de informațiile disponibile.

8. Forța majoră

Niciuna dintre părți nu va fi răspunzătoare pentru neexecutarea obligațiilor sale contractuale dacă aceasta este cauzată de forța majoră.

9. Litigii

Orice litigiu apărut între părți în legătură cu prezentul contract va fi soluționat pe cale amiabilă. În cazul în care nu se ajunge la o soluționare amiabilă, litigiul va fi soluționat de instanța judecătorească competentă.

10. Modificări

Prezentul contract poate fi modificat numai prin acordul scris al părților.

11. Durata și încetarea contractului

Prezentul contract se încheie pe o perioadă de .....ani și poate fi prelungit prin acordul scris al părților.
Prezentul contract încetează în următoarele situații:

a. la expirarea duratei de valabilitate;
b. prin acordul scris al părților;
c. prin denunțarea unilaterală a contractului de către una dintre părți, cu o notificare prealabilă de ....

Încheiat în două exemplare, câte unul pentru fiecare parte, astăzi .....

Pentru Spitalul "Maria"	**Pentru iQuality Services**
.....	.....

OBLIGAȚII PRIVIND TRANSPARENȚA ȘI INFORMAREA

MESAJUL DE AVERTIZARE (EXEMPLU)

iQUALITY SERVICES

iQuality Services

Piața 1 Decembrie 1918, 24, Reșița

+40 725 631 096

www.ioniordache.com

ion@ioniordache.com

Pentru mai multe informații vă invităm să studiați politica de confidențialitate disponibilă pe site.

Scopul, categoriile de date, temeiurile prelucrării și perioada de stocare.
În conformitate cu dispozițiile LEGII nr. 333 din 2003 (**republicată**)(*actualizată*) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor şi ale HOTĂRÂRII nr. 301 din 2012(*actualizată*) pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333 avem obligația de a stoca înregistrările video ale persoanelor care tranzitează zona căilor de acces, în vederea asigurării pazei și protecției bunurilor și persoanelor aflate în incinta sediului nostru. Vom stoca datele pentru maxim 20 de zile.

Destinatarii datelor cu caracter personal
Pentru situații excepționale sau atunci când legea prevede, datele pot fi divulgate sau puse la dispoziția unor terțe persoane (spre exemplu, societății care prestează serviciu de pază și intervenție rapidă), autorităților, instituțiilor, organelor publice, pentru respectarea unei cerințe legale sau pentru protejarea drepturilor și activelor societății noastre sau ale altor entități sau persoane, precum instanțele de judecată.

Securitatea prelucrării datelor
Am luat măsuri tehnice și organizatorice adecvate, pentru protejarea datelor cu caracter personal, împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii, accesului neautorizat sau oricărei alte forme de prelucrare ilegală.
Evaluăm și actualizăm constant măsurile de securitate implementate pentru a asigura condiții optime de securitate a datelor tale.

Drepturile tale
Conform Regulamentul general privind protecția datelor (GDPR) beneficiați de dreptul de acces, de intervenție asupra datelor, dreptul de opoziție, dreptul de a nu fi supus unei decizii individuale, dreptul de a depune plângere în fața Autorității de Protecție a Datelor și dreptul de a vă adresa justiției. Aceste drepturi pot fi exercitate în orice moment.
Pentru exercitarea acestor drepturi, vă încurajăm să adresați o solicitare în scris, datată și semnată, la sediul nostru sau prin e-mail, utilizând datele de contact de mai sus.

METODOLOGIA
GDPR VIDEOSHIELD

iQuality Services

PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIN MIJLOACE VIDEO

CONFORM REGULAMENTULUI (UE) 679/2016
Regulamentul General privind Protecția Datelor (RGPD)

Consultanță în elaborarea următoarelor documente:

- **Politica** de prelucrare a datelor cu caracter personal prin mijloace video.
- **Evaluarea** de impact privind prelucrarea datelor cu caracter personal pentru sistemul de supraveghere video.
- **Informarea** privind prelucrarea datelor cu caracter personal prin intermediul sistemului de supraveghere video.
- **Procesul verbal** de consultare a reprezentanților salariaților referitor la supravegherea video în interesul legitim al angajatorului.
- **Afișul** de atenționare/informare privind monitorizarea video.
- **Lista** cu persoanele care au acces la spațiile în care sunt prelucrate date personale.
- **Chestionar** de evaluare a persoanei împuternicite de operator
- **Acord** cu persoana împuternicită de operator privind prelucrarea datelor cu caracter personal conform Art.28 din GDPR.

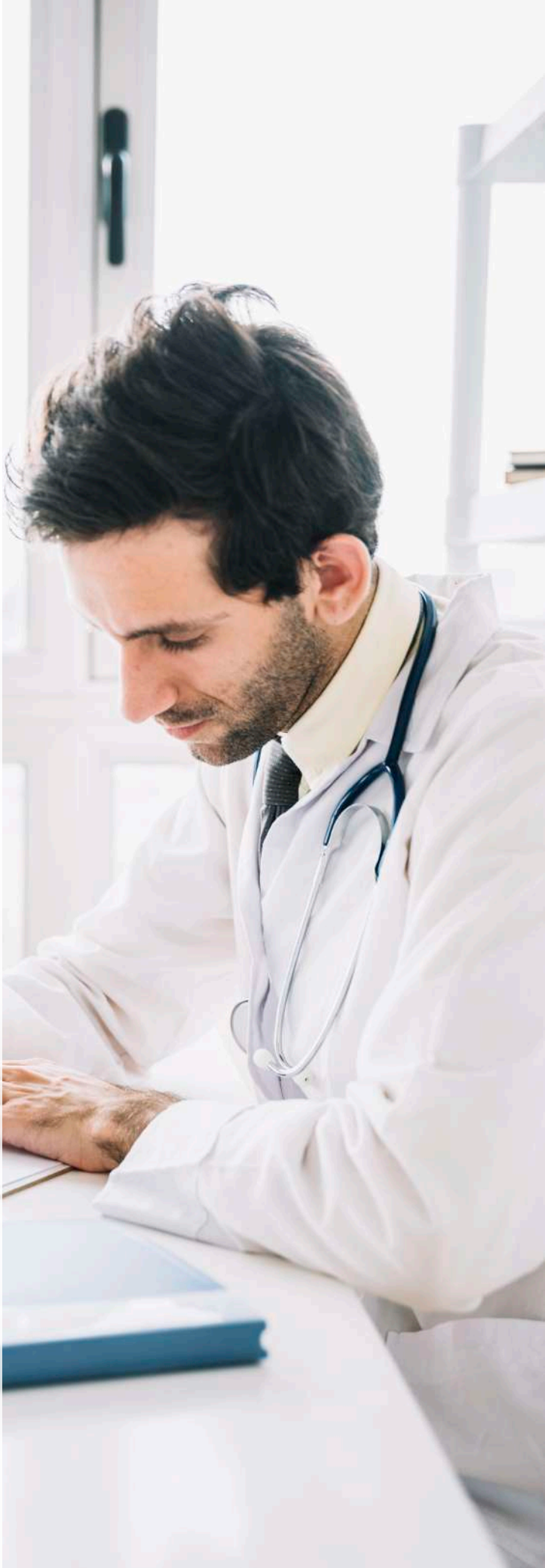
- **Audit** pentru stabilirea gradului inițial de conformitate privind prelucrarea datelor cu caracter personal prin mijloace video.
- **Conștientizarea** personalului prin sesiuni de prezentare a „Ghidului 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video", Comitetul European pentru Protecția Datelor.
- **Instruirea** personalului implicat în prelucrarea datelor cu caracter personal pentru conformarea la GDPR, atat general cât și pentru operarea proceselor specifice pe funcțiuni.

www.ioniordache.com
ion@ioniordache.com
+40 (725) 631 096

CAPITOLUL 11

INTERVIURI CU MANAGERI AI UNITĂȚILOR SANITARE

În acest capitol vă prezentăm interviuri cu manageri ai unităților sanitare care ne arată cum abordează ei, în unitățile lor sanitare problemele legate de securitate și siguranță.



INTERVIURI
CU MANAGERI AI UNITĂȚILOR SANITARE

În călătoria noastră către înțelegerea și promovarea securității și siguranței în cadrul unităților sanitare, ne îndreptăm acum atenția către vocile și experiența liderilor care conduc aceste instituții vitale.

În cadrul acestui capitol, vom avea privilegiul de a învăța de la managerii unor unități sanitare diverse - spitale, clinici, cabinete medicale individuale și altele.

Securitatea și siguranța reprezintă aspecte esențiale pentru funcționarea cu succes a oricărei unități sanitare, indiferent de dimensiune sau specific. În contextul actual, marcat de numeroase evoluții tehnologice, sociale și legislative, provocările în ceea ce privește asigurarea unui mediu sigur și securizat sunt în continuă schimbare. Prin urmare, este important ca decidenții și managerii din domeniul sanitar să fie mereu la curent cu noile riscuri care pot apărea și cu cele mai bune practici de gestionare a acestora.

Scopul acestui capitol este de a evidenția importanța acordată de managerii unităților sanitare securității și siguranței, precum și de a împărtăși perspective unice asupra modului în care aceste aspecte se încadrează în misiunea generală a fiecărei instituții. Managerii sunt lideri cheie în eforturile de asigurare a unui mediu sigur și securizat pentru pacienți, personal medical și bunurile instituției. Cu experiența și viziunea lor, contribuie la modelarea strategiilor și a culturii de securitate în unitățile lor.

Interviurile cu managerii unităților sanitare au fost concepute pentru a adresa patru întrebări esențiale, identice pentru toți respondenții. Aceste întrebări au fost selectate cu atenție pentru a dezvălui perspectivele individuale ale managerilor și pentru a evidenția aspecte critice ale securității și siguranței în cadrul unităților sanitare.

Cele patru întrebări adresate acoperă o gamă largă de subiecte relevante, de la viziunea managerilor asupra rolului securității, la cultura organizațională privind siguranța și exemple concrete de bune practici adoptate cu succes.

Iată principalele obiective ale acestor întrebări:

1. Rolul securității și siguranței în misiunea unității sanitare

Prima întrebare vizează viziunea managerilor cu privire la rolul securității și siguranței în instituția lor. Dorim să înțelegem cum percepe fiecare manager aceste aspecte și cum le integrează în misiunea generală a unității. Răspunsurile la această întrebare vor sublinia importanța acordată acestor aspecte de către manageri și modul în care acestea influențează serviciile medicale oferite și satisfacția pacienților.

2. Provocările majore de securitate și măsurile de gestionare

A doua întrebare are ca scop explorarea provocărilor majore de securitate cu care se confruntă fiecare unitate sanitară și a măsurilor luate pentru a le gestiona. Cu această întrebare, ne dorim să evidențiem varietatea problemelor de securitate specifice fiecărui tip de unitate sanitară și strategiile aplicate pentru a le aborda.

3. Cultura de securitate a personalului și măsuri pentru îmbunătățire

A treia întrebare se concentrează pe cultura de securitate a personalului din unitatea sanitară. Înțelegem că securitatea nu este doar o chestiune tehnică, ci și o chestiune culturală. Vrem să aflăm cum percep și se angajează angajații în practicile de securitate și ce măsuri s-au implementat sau se intenționează să se implementeze pentru a îmbunătăți această cultură.

4. Soluții de securitate eficiente

Ultima întrebare ne oferă oportunitatea de a explora soluțiile de securitate implementate în unitățile sanitare și eficacitatea acestora. Dorim să evidențiem bunele practici și inovațiile care au dat rezultate pozitive în fiecare instituție. Managerii vor împărtăși lecții învățate și rezultatele observate, oferind astfel exemple de succes care pot inspira și ajuta alte unități să își îmbunătățească securitatea.

Cum vedeți rolul securității și siguranței în cadrul unității sanitare pe care o gestionați și cum se încadrează acesta în misiunea generală a unității?

Prima întrebare se referă la viziunea dvs. asupra rolului securității și siguranței în cadrul unității sanitare pe care o administrați.

Înțelegem că fiecare instituție medicală are o misiune unică și o serie de obiective specifice. Siguranța și securitatea pot părea elemente de suport, dar în realitate, acestea sunt componente esențiale care contribuie la funcționarea eficientă și de succes a unității dumneavoastră.

Obiectivul acestei întrebări este de a sublinia înțelegerea și valorizarea pe care o acordați securității și siguranței în cadrul instituției pe care o conduceți.

Vrem să înțelegem cum se încadrează aceste aspecte în misiunea generală a unității dumneavoastră și cum acestea influențează direct serviciile medicale oferite și satisfacția pacienților.

De asemenea, acesta este un moment în care puteți împărtăși experiențe sau inițiative proprii care au consolidat securitatea și siguranța în cadrul unității sanitare.

Apreciem viziunea dvs. unică și așteptăm cu nerăbdare să înțelegem mai bine cum se reflectă aceasta în strategia dvs. de securitate.

Această întrebare poate să scoată în evidență viziunea fiecărui manager privind securitatea și să evidențieze rolul său central în funcționarea unității sanitare.

"Securitatea și siguranța ocupă un rol central în cadrul clinicii noastre, Dentcof. Considerăm că aceste aspecte sunt fundamentale pentru furnizarea de servicii medicale de calitate și pentru satisfacția pacienților noștri.

Misiunea noastră este să oferim servicii stomatologice de înaltă calitate, într-un mediu sigur și confortabil, pentru a promova sănătatea orală și bunăstarea pacienților noștri.

De altfel, suntem dedicați protejării confidențialității pacienților și a datelor lor medicale, astfel ca am implementat sisteme avansate de securitate cibernetică pentru a proteja informațiile lor sensibile."

Mădălina Nicolin,
Manager General
Clinica Dentcof, Timișoara

"În unitatea noastră sanitară, securitatea și siguranța sunt priorități de top.

Rolul lor este de a proteja atât persoanele (pacienții, personalul medical, vizitatorii), cât și bunurile (echipamente, datele pacienților, activele instituției).

Așadar, securitatea și siguranța sunt strâns legate de misiunea noastră de a oferi servicii medicale de înaltă calitate, într-un mediu sigur și securizat."

Dr. Caius Diaconescu,
Medic Primar Diabet Zaharat, Nutriție, Boli Metabolice
Sef Secție - Spitalul Județean de Urgență Reșița

"Securitatea și siguranța sunt elemente principale în unitatea sanitară pe care o coordonez.

Ele sunt esențiale în procesul de sănătate pe care îl oferim.

Nu doar securitatea echipamentelor medicale și a bunurilor sunt importante, consider că un factor principal este acela de a crea pacienților noștrii un sentiment de siguranță în unitatea medicală, acesta fiind și scopul nostru."

Dr. Ștefania Șerban,
Manager
Spitalul CFR Sibiu

Care sunt provocările majore de securitate cu care se confruntă unitatea dvs. sanitară în prezent și ce măsuri ați luat pentru a le gestiona?

A doua întrebare se concentrează asupra provocărilor majore de securitate cu care se confruntă unitatea dumneavoastră sanitară și asupra modului în care acestea sunt gestionate.

Securitatea în cadrul unităților sanitare poate fi o problemă complexă și multifacțională, implicând o multitudine de riscuri potențiale - de la protecția datelor până la siguranța pacienților și a personalului.

Scopul acestei întrebări este de a capta varietatea provocărilor de securitate specifice fiecărui tip de unitate sanitară și de a ilustra strategiile aplicate pentru a le gestiona.

Înțelegem că fiecare unitate sanitară are un set unic de provocări, bazate pe o multitudine de factori, precum dimensiunea instituției, localizare, serviciile oferite, resursele disponibile și multe altele.

În plus, prin abordarea acestei întrebări, ne dorim să înțelegem mai bine cum ați reușit să navigați prin aceste provocări și să vă adaptați în vederea asigurării unui mediu sigur și securizat.

Experiența și înțelegerea dumneavoastră pot oferi o perspectivă prețioasă pentru ceilalți lideri din domeniul sănătății și pot contribui la îmbunătățirea continuă a standardelor de securitate în întregul sector.

"În clinica noastră suntem implicați cu toții în securitatea și siguranța fizică, și în securitatea datelor. Considerăm că acestea sunt aspecte critice, iar pentru a le aborda, am identificat mai multe provocări majore.

Având în vedere specificul activității noastre, cu o pondere ridicată a aplicațiilor digitale integrate, în care prelucrăm un volum mare de date ale pacienților, protecția acestora a devenit o preocupare principală.

De asemenea, siguranța personalului și a pacienților prezintă o importanță critică. Am dezvoltat protocoale stricte pentru prevenirea accidentelor și incidentelor, coroborat cu integrarea unei infrastructuri de supraveghere video, antiefracție și control acces."

Mădălina Nicolin,
Manager General
Clinica Dentcof, Timișoara

"Una dintre cele mai mari provocări de securitate cu care ne confruntăm în unitatea noastră sanitară este protecția datelor pacienților. În era digitală, este vital să protejăm informațiile sensibile și confidențiale ale pacienților împotriva amenințărilor cibernetice.
Am luat măsuri concrete pentru a ne proteja datele, inclusiv implementarea de protocoale stricte de securitate a datelor, instruirea personalului nostru cu privire la practicile de securitate cibernetică și angajarea unei firme de securitate cibernetică pentru a monitoriza și a apăra rețeaua noastră."

Dr. Caius Diaconescu,
Medic Primar Diabet Zaharat, Nutriție, Boli Metabolice
Sef Secție - Spitalul Județean de Urgență Reșița

"Securitatea fizică a pacienților, a personalului medical și a echipamentelor medicale este o provocare zilnică la care noi trebuie să răspundem.
Dat fiind numărul mare de vizitatori am implementat măsuri de securitate prin pază umană și sisteme de control acces astfel încât persoanele care acced în unitate să fie cunoscute de către personal și să nu aibă acces în zonele cu risc din cadrul unității."

Dr. Ștefania Șerban,
Manager
Spitalul CFR Sibiu

Cum ați descrie cultura de securitate a personalului din unitatea dvs. sanitară și ce pasi ați luat sau intenționați să luați pentru a o îmbunătăți?

A treia întrebare referă la cultura de securitate existentă în cadrul unității dumneavoastră sanitare.

Este important să înțelegem că securitatea și siguranța nu sunt doar rezultatul tehnologiei sau al regulilor stricte, ci reprezintă și un produs al culturii organizaționale, care se reflectă în atitudinile și comportamentul angajaților.

Prin această întrebare, ne propunem să explorăm modul în care angajații dumneavoastră percep și se angajează în practicile de securitate, precum și strategiile pe care le-ați implementat sau intenționați să le implementați pentru a îmbunătăți această cultură de securitate.

Înțelegerea nivelului de conștientizare a securității și angajamentul față de aceasta ne va ajuta să obținem o imagine mai completă a modului în care securitatea este încorporată în mod activ în viața de zi cu zi a unității sanitare. De asemenea, ne va ajuta să identificăm strategii eficiente de promovare a unei culturi puternice de securitate, care pot fi împărtășite cu alte unități sanitare.

Această întrebare ar putea să evidențieze gradul de importanță pe care angajații îl acordă securității și siguranței, precum și măsurile manageriale de a promova această cultură.

"Cultura de securitate în cadrul clinicii noastre este solidă, cu un accent deosebit pe conștientizarea și educația personalului cu privire la securitate, iar scopul nostru este să asigurăm un mediu sigur pentru pacienți și personal.

Dat fiind faptul ca interactionam deseori cu pacienți străini, iar o mare parte din comunicarea cu pacienții noștri, dar și comunicarea în cadrul echipei medicale, referitoare la cazurile medicale, se realizează digital, angajații noștri înțeleg în mod profund importanța securității și siguranței, atât a datelor, cât și a siguranței fizice."

Mădălina Nicolin,
Manager General
Clinica Dentcof, Timișoara

"Cultura de securitate este o componentă fundamentală a eticii profesionale în unitatea noastră sanitară. Personalul nostru înțelege și apreciază necesitatea de a menține un mediu sigur și securizat pentru toți pacienții și vizitatorii.

Cu toate acestea, pentru a ne îmbunătăți și mai mult cultura de securitate, vom introduce programe de formare și sensibilizare mai cuprinzătoare, iar acestea vor acoperi o gamă mai largă de teme, de la prevenirea furtului la protecția împotriva amenințărilor cibernetice."

Dr. Caius Diaconescu,
Medic Primar Diabet Zaharat, Nutriție, Boli Metabolice
Sef Secție - Spitalul Județean de Urgență Reșița

"Cultura de securitate în unitatea noastră sanitară este un factor foarte important care necesită implicarea întregului personal.

Fiecare angajat al nostru înțelege acest aspect și respectă procedurile de securitate.

În vederea îmbunătățirii măsurilor de securitate am demarat externalizarea serviciilor de pază, monitorizare și intervenție."

Dr. Ștefania Șerban,
Manager
Spitalul CFR Sibiu

Care sunt cele mai eficiente soluții de securitate pe care le-ați implementat în unitatea dumneavoastră sanitară și care au fost rezultatele acestora?

A patra și ultima întrebare se referă la soluțiile de securitate pe care le-ați implementat în unitatea dumneavoastră sanitară și eficiența acestora.

Acesta este un aspect esențial, deoarece ne ajută să înțelegem care sunt măsurile concrete pe care le-ați luat pentru a asigura securitatea și siguranța și cum acestea au influențat efectiv unitatea dumneavoastră.

Obiectivul acestei întrebări este de a scoate în evidență bunele practici în ceea ce privește securitatea și siguranța în unitățile sanitare și de a oferi oportunitatea de a împărtăși cu ceilalți modele de succes și inovații. Ne interesează soluțiile care s-au dovedit a fi eficiente în contextul specific al unității dumneavoastră și care ar putea servi drept inspirație sau punct de referință pentru alte unități.

Vă invităm să împărtășiți experiențele dvs. pozitive, lecțiile învățate și rezultatele observate. Răspunsurile dumneavoastră ar putea avea un impact semnificativ asupra modului în care alți manageri de unități sanitare percep și abordează securitatea și siguranța în propriile lor instituții.

Aceasta ar permite managerilor să evidențieze exemple de bune practici și ar putea oferi cititorilor un model sau inspirație pentru îmbunătățirea securității în propriile lor unități.

"În cadrul clinicii Dentcof, am implementat mai multe soluții de securitate eficiente, iar acestea au adus rezultate semnificative în asigurarea unui mediu sigur pentru pacienți și personal.

Investiția în sisteme de securitate avansate, menite a proteja datele sensibile ale pacienților și ale clinicii noastre ne-a ajutat la prevenirea accesului neautorizat și a scurgerii de date.

De asemenea, am instalat sisteme de supraveghere video în zonele cheie ale clinicii."

Mădălina Nicolin,
Manager General
Clinica Dentcof, Timișoara

"Una dintre cele mai eficiente soluții de securitate pe care le-am implementat este un sistem eficient de control al accesului. Acesta necesită ca personalul și vizitatorii să utilizeze carduri de acces pentru a intra în anumite zone ale clădirii noastre.

De asemenea, am îmbunătățit iluminatul și supravegherea video în întreaga unitate. Rezultatul a fost o reducere semnificativă a incidentelor de securitate și o îmbunătățire a sentimentului general de siguranță pentru pacienți și personal."

Dr. Caius Diaconescu,
Medic Primar Diabet Zaharat, Nutriție, Boli Metabolice
Sef Secție - Spitalul Județean de Urgență Reșița

"Am investit in securitatea unității noastre prin contractarea unei firme de pază, pentru a gestiona accesul persoanelor în spital și clădirea administrativă, prin identificarea acestora la intrare și consemnarea lor într-un registru, pentru a avea o evidență clară a persoanelor ce vizitează unitatea, indeferent de scop.

Acest lucru este dublat de existența la nivelul clădirii spitalului a ușilor cu control acces pe baza de cartelă electronică și/sau cod unic personalizat al angajatului, obținându-se astfel și o evidență a accesului personalului în diferite sectoare ale spitalului, cu restricții în zonele cheie (cabinete medici, bloc operator, ATI) în funcție de tipul de personal."

Dr. Ștefania Șerban,
Manager
Spitalul CFR Sibiu

BIBLIOGRAFIE

- **LEGEA nr. 333 din 8 iulie 2003 (republicată) privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor**.
- **HOTĂRÂREA nr. 301 din 11 aprilie 2012 (republicată) pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor**.
- **INSTRUCŢIUNILE nr. 9 din 1 februarie 2013 privind efectuarea analizelor de risc la securitatea fizică a unităţilor ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor**.
- **Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).**
- **Hospital and Healthcare Security 6th Edition,** by Tony W. York & Don MacAlister
- **Security Management for Healthcare: Proactive Event Prevention and Effective Resolution**, 1st Edition, by Bernard Scaglione
- **Healthcare Security: Solutions for Management, Operations, and Administration**, 1st Edition, by Anthony Luizzo & Bernard J. Scaglione
- **Effective Security Management**, 7th Edition, by Charles A. Sennewald & Curtis Baillie
- **The Security Guidelines, Queensland Health 2022** ('the guidelines'), by Queensland Government (Australia)
- **Security Design Guidelines for Healthcare Facilities**, by International Association for Healthcare Security and Safety (IAHSS)
- **CPTED and Traditional Security Countermeasures: 150 Things You Should Know**, by Lawrence Fennelly & Marianna Perry
- **21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Second Edition**, by Randall I. Atlas
- **Prevenirea incendiilor la unităţi sanitare şi de îngrijire**, Inspectoratul pentru Situații de Urgență "Dobrogea" al judetului Constanța
- **LEGEA nr. 307/2006 privind apărarea împotriva incendiilor** (actualizată)
- **ORDINUL nr. 146 din 24 octombrie 2013 pentru aprobarea Dispoziţiilor generale de apărare împotriva incendiilor la unităţi sanitare**, EMITENT: MINISTERUL AFACERILOR INTERNE Nr. 146 din 24 octombrie 2013, MINISTERUL SĂNĂTĂŢII Nr. 1.427 din 26 noiembrie 2013 PUBLICAT ÎN: MONITORUL OFICIAL nr. 758 din 5 decembrie 2013
- **Manager de securitate**, suport de curs, RQM Certification
- **Managementul operațiunilor de securitate**, suport de curs, RQM Certification

Două instrumente de inteligență artificială au fost folosite pentru a adăuga un nivel suplimentar la procesul de editare a acestui ghid:

- **ChatGPT** (Chat Generative Pre-trained Transformer), OpenAI, Microsoft Corporation
- **Claude 2**, https://www.anthropic.com

RQM CERT

Your Knowledge Provider

RQM Cert este un furnizor de formare profesională cu o echipă de specialişti cu experienţă în servicii de pregătire profesională, evaluare şi audit. Avem cunoştinţe în sisteme de management al calităţii, mediu, sănătate şi siguranţă ocupaţională, auto, securitate fizică, a informaţiilor, protecţiei datelor şi serviciilor IT.

Programele noastre de formare sunt concepute pentru a sprijini învăţarea activă în conformitate cu standardele internaţionale şi cerinţele specifice industriei.

DOMENIILE NOASTRE DE FORMARE

- ❑ Security & Fire Protection
- ❑ Automotive
- ❑ Project Management
- ❑ Service Management
- ❑ Information Security
- ❑ Cybersecurity
- ❑ Continuity, resilience, and recovery
- ❑ Governance, risk, and compliance
- ❑ Privacy and Data Protection
- ❑ Quality and Service Management
- ❑ Health and Safety
- ❑ Sustainability
- ❑ Cloud Credential Council (CCC)

Classroom Training

RQM Cert deliver high-quality worldwide classroom trainings at various locations.

Self-study Training

Self-studying is an excellent way to highlight personal drive and intellectual curiosity when applying to training courses.

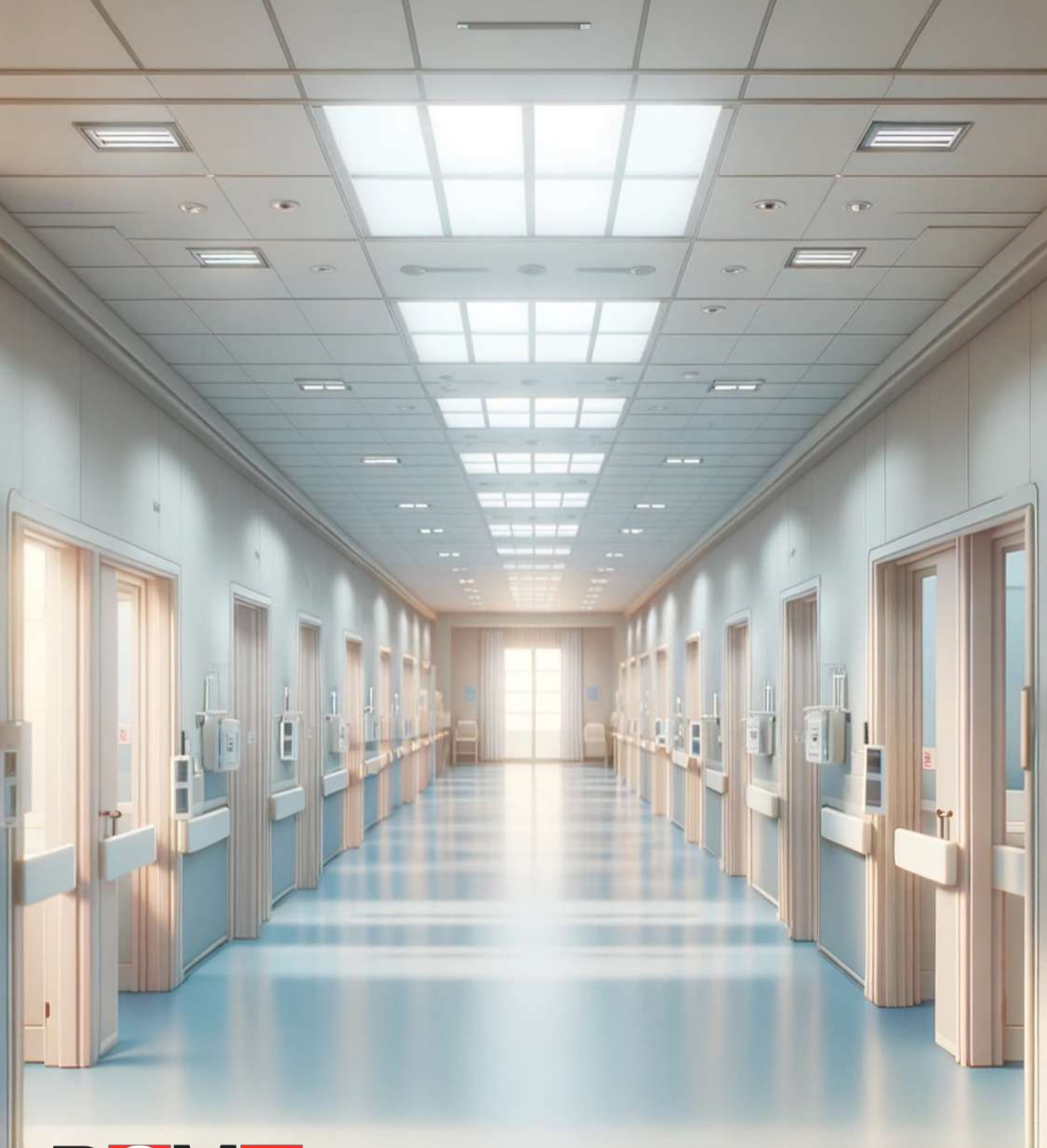
In-House Training

RQM Cert provides woldwide in-house courses, delivered by our trainers directly at your facility.

Virtual Classroom

Our Virtual Classroom training is the perfect method for you to participate in highly valuable learning from anywhere in the world to enhance skills.

CONTACT: +40 356 173 020 www.rqmcert.com office@rqmcert.com



RQM CERT
Your Knowledge Provider

www.rqmcert.com
office@rqmcert.com
+40 356 173 020

RQM Certification cu sediul în Timișoara este un furnizor de formare profesională cu o echipă excepțională de specialiști cu mare experiență în formare profesională, servicii de evaluare și audit.

Compania are expertiză în domeniul sistemelor de management al calității, al mediului, al sănătății și securității la locul de muncă, al automobilelor, al securității fizice, al informațiilor și al serviciilor IT.

Programele de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice fiecărei industrii.

GHID ILUSTRAT - SECURITATEA ȘI SIGURANȚA UNITĂȚILOR SANITARE