ИНФОРМАЦИОННАТА СИГУРНОСТ В ЛЕЧЕБНИТЕ ЗАВЕДЕНИЯ. МЕРКИ ЗА ПОДОБРЯВАНЕТО Й

ас. д-р Йордан Георгиев Деливерски[*]
Университет по библиотекознание и информационни технологии

INFORMATION SECURITY IN MEDICAL INSTITUTIONS. MEASURES FOR IMPROVEMENT

Assist. Prof. Jordan Georgiev Deliversky, PhD[*]
State University Of Library Studies And Information Technologies

***Резюме**: Въвеждането на информационни системи в лечебните заведения има висок потенциал за подобряване на достъпността на клиничната информация, както и за подобряване на здравните грижи. Въпреки това използването на информационните технологии в здравеопазването, води до множество предизвикателства свързани с информационната сигурност.*
Най-често срещаните трудности по отношение на опазване на информационната сигурност са свързани с поверителността и предотвратяване на неоторизирания достъп до клинични данни на пациентите.
Всички служители в лечебните заведения трябва да бъдат обучени по отношение принципите на информационната сигурност. Всички те трябва да бъдат запознати с техните отговорности за защита на информацията.
Пациентската информация съдържаща се в болничните информационни системи е чувствителна и строго поверителна, като защитата й е от съществено значение. Нерегламентираният достъп и разгласяването на информация свързана със живота и здравето на пациента може да има етични, социални и съдебни последици.

***Ключови думи**: информационни системи, лечебни заведения, информационна сигурност*

***Abstract:** The introduction of information systems in medical institutions has high potential to improve the accessibility of clinical information and to improve health care. However, use of information technology in health care leads to many challenges related to information security.*
The most common difficulties in protecting information security are related to confidentiality and prevention of unauthorized access to patients' clinical data.
All employees in medical institutions should be trained in the principles of information security. They all need to be aware of their responsibilities to protect the information.

[*] Доктор по „Организация и управление извън сферата на материалното производство", Катедра „Национална сигурност" , УНИБИТ, e-mail: deliversky@yahoo.com
[*] Doctor of Philosophy (Ph.D.), Organization and Management Outside the Sphere of Material Production, Department of National Security, State University of Library Studies and Information Technologies, Sofia, Bulgaria, e-mail: deliversky@yahoo.com

Patient information contained in hospital information systems is sensitive and highly confidential, and its protection is essential. Unauthorized access and disclosure of information related to the life and health status of patients may have ethical, social and legal consequences.

***Key words**: Information systems, medical institutions, information security*

Въвеждането на информационни системи в лечебните заведения има висок потенциал за подобряване на достъпността на клиничната информация, както и за подобряване на здравните грижи. Въпреки това използването на информационните технологии в здравеопазването, води до множество предизвикателства свързани с информационната сигурност.

Информационните технологии са компютърни и телекомуникационни технологии, които осигуряват автоматизирани методи за обработка на информацията. Информационните системи са системи от човешки и технически компоненти, които приемат, съхраняват, обработват, предоставят и прехвърлят информация. Те могат да бъдат базирани на различни комбинации между човешките усилия, и информационните технологии.

Към настоящия момент лечебните заведения не само предоставят здравни услуги, но също така се конкурират помежду си не само за постигане на добър финансов резултат, но и за постигане на висок рейтинг и акредитация. Един от подходите за постигане на подобряването на здравните грижи е използването на информационни технологии и информационни системи[1]. Надеждната и достоверна информация трябва да бъде идентифицирана, събрана и разпространена в подходяща форма и срокове, като по този начин всяко едно длъжностно лице в лечебното заведение да може да поема определена отговорност. Информационните системи осигуряват оперативна, финансова, законодателна и друг вид информация и данни, които подпомагат управлението и контрола върху дейността на лечебните заведения.

Информационните системи в болничните заведения се използват широко във връзка с приключване на дневните задачи от страна на медицинския и немедицински персонал, за комуникацията между различните отделения или отдели в лечебното заведение, както и за комуникация с институции и организации извън лечебното заведение. В най-общ смисъл използването на болничните информационни системи има редица предимства както за предоставящите, така и за получаващите здравна услуга/грижа. Тези системи имат сериозен потенциал свързан както с увеличаване на достъпността до клинична информация така и за подобряване на изследванията за клиничното и обществено здраве. Въпреки това използването на информационните системи води до нови предизвикателства свързани с информационната сигурност на тези системи.

Най-често срещаните трудности по отношение на опазване на информационната сигурност са свързани с поверителността и предотвратяване на неоторизирания достъп до клинични данни на пациентите. От една страна информацията за пациентите е изключително чувствителна и е необходимо да бъде запазена сигурна и поверителна, като от друга страна различни доставчици на здравни услуги/грижи е необходимо да имат достъп до тях.

Лечебните заведения събират, използват и съхраняват лични данни и клинична информация. По тази причина рисковете от изтичане на информация и нарушаване на правото на неприкосновеност на личния живот, може да доведе до последствия

много по-тежки отколкото при други организации. По тази причина трябва да се обърне особено внимание на въпросите свързани със сигурността на информацията, в съответствие с правилата за информационна сигурност и законовите актове[2].

Всички служители в лечебните заведения трябва да бъдат обучени по отношение принципите на информационната сигурност. Всички те трябва да бъдат запознати с техните отговорности за защита на информацията. Новоназначените служители трябва да бъдат включвани в обучения за повишаване на знанията в качеството им на потребители на информационните системи в лечебните заведения, с оглед постигане добро ниво на информационна сигурност. В противен случай, липсата на обучение, липсата на инструкции за управление и поведение по въпросите свързани със сигурността, както и липсата на ясни и документирани политики за справяне с рисковите фактори, може да създаде проблеми за работниците и служителите в лечебните заведения. За да се изследва информационната сигурност в лечебните заведения, следва да се обърне внимание на три основни типа предпазни мерки – физически, технически и административни[3].

- Физическите предпазни мерки са вързани със способността на организацията да се защити от физически заплахи. Тези предпази мерки гарантират, че медицинския персонал ще получи достъп до защитената медицинската информация, така че да може да продължи да предоставя медицински услуги/грижи, когато това е необходимо;
- Техническите предпазни мерки са свързани най-общо с предпазване от електронни заплахи за медицинската информация. Най-често те са свързани с:
  - Осигуряване на технически политики и процедури, които позволяват на упълномощени служители да получат достъп до информационните системи в лечебните заведения;
  - Технически мерки за сигурност, защита и предотвратяване на неоторизиран достъп до информационните системи;
  - Въвеждане на контроли свързани със защитата и невъзможността да бъде променяна или повреждана медицинската информация.
- Мониторинг /чрез софтуер или хардуер/ или процедурни механизми свързани със записване и разглеждане на всички записи и промени реализирани в информационните системи;
- Административните предпазни мерки се фокусират върху вътрешната организация. Върху политиките и процедурите касаещи мерките за сигурност които защитават здравната информацията за пациента.

Докато физическите предпазни мерки предпазват лечебните заведения от физическа кражба или повреда, а техническите я защитават от електронна заплаха, то административните предпазни мерки създават здравата основа за сигурност.

Основните цели на информационната сигурност включват поддържане на конфиденциалност, достъпност и интегритет на информацията, като в сферата на здравеопазването, сигурността на защитаваните обекти зависи от запазването на конфиденциалност на информацията свързана със здравния статус на пациента. С оглед запазването на конфиденциалността, следва да бъдат предприети мерки за гарантиране на интегритета на информацията, тъй като е възможно да бъде нарушена целостта на данните, контрола на достъп и способите за мониторинг и контрол на системата, както и друг вид системна информация, което би довело до нарушаване на поверителността, а това понякога може да остане незабелязано. Невъзможността за гарантиране на сигурността на информацията в системата, може да даде възможност за манипулиране на данни от здравните досиета на пациентите, което би причинило вреда на па-

циента, тъй като не може да се предприемат адекватни мерки от страна на медицинския персонал за постигане на благоприятен терапевтичен резултат.

По същия начин, високото ниво на надеждност е особено важно за информационните системи в лечебните заведения, където при лечението на пациентите факторът време е от критична важност по отношение на вземането на решения. В действителност кризи свързани с фактори, които нямат отношение към здравните аспекти на информацията съдържаща се в информационните системи на лечебните заведения, могат да имат изключително негативно влияние върху цялата система. От друга страна, особено често явление е наличието на атаки спрямо системите, които не позволяват на потребителите да използват функционалностите на системата с което се възпрепятства възможността за работа и използване на ресурсите на информационната система.

Минималните изисквания за мониторинг на информационните системи трябва да са съобразени със специфичните изисквания свързани със здравеопазването и да са формулирани по начин даващ възможност да се предпази наличността, целостта и конфиденциалността на личната здравна информация и да се гарантира, че достъпа до такава информация може да бъде контролиран и одитиран. По този начин мониторинга на системата помага за предотвратяване на грешки свързани с медицинската практика, които могат да произтекат от некоректна /компрометирана/ здравна информация съдържаща се в информационните системи. По този начин си подпомага възможността да се гарантира непрекъснатост на предоставяните медицински услуги.

При формирането на целите свързани с информационната сигурност в здравеопазването има допълнителни съображения, които[4]:

- произтичат от законодателството. Изразяват се в съобразяване с нормативни изисквания свързани със защита правата на пациентите и защита на личните данни. Тук се включват и правила за етично поведение заложени в Етичните кодекси на лечебните заведения, на съсловните организации и на Световната здравна организация. Тези етични стандарти оказват пряко влияние върху формирането на политиката за информационна сигурност в лечебните заведения.
- са свързани с поддържане и установяване на добри практики за сигурност и поверителност в информационните технологии в сферата на здравеопазването;
- са свързани с поддържане на високо ниво на отчетност, както по отношение на отделните служители, така и на ниво организация;
- са свързани с прилагане, поддържане и подкрепа на система за управление на риска в организацията;
- са свързани със задоволяване на базовите потребности от сигурност при обичайната работа в лечебните заведения;
- са свързани с намаляване на оперативните разходи, чрез внедряване и широко използване на сигурни информационни технологии, по начин по който не се ограничават обичайните дейности свързани с оказване на здравни грижи.
- са свързани с наличие и поддържане на обществено доверие в здравните организации и ползваните от тях информационни технологии;
- са свързани със спазване на професионални стандарти и етични правила установени от съсловните организации, с оглед гарантиране поверителността на здравната информация;
- са свързани със създаване на безопасна среда за сигурност за информационната система, изолирана от външни заплахи;

- са свързани с установяване на оперативна съвместимост по отношение на информацията в различните информационни системи както в лечебното заведение, така и между различните организации. Оперативната съвместимост подобрява правилното подаване и интерпретиране на здравната информация за да се гарантира цялостността, достъпността и поверителността й.

Пет са основните направления свързани с постигането на добро ниво на информационна сигурност в лечебните заведения [5]:

1. **Премахване на споделените потребителски акаунти.** Обичайна практика е лекари в едно лечебно заведение, както и членове на медицинския и немедицински персонал да използват общи потребителски акаунти с един набор от идентификационни данни за информационните системи /потребителско име и парола/. Основна причина за това споделяне е за да се спести време при изход или вход в информационната система. Ползването обаче на такъв общ, незащитен потребителски акаунт може да доведе до нерегламентиран достъп и изтичане на поверителна информация. За да се избегне този проблем всички лекари, медицински сестри и друг немедицински персонал се нуждаят от собствени потребителски акаунти за вход и идентификация в информационната система. Системата трябва да е разработена по начин, който да предоставя нужната информация, като предоставя достъп до точно определен набор от документи за всяко заинтересовано лице. Възможност за вход и идентификация в системата е наличието на смарткарти, чрез които да се идентифицира всеки потребител чрез прекарване на всяка карта през четец.

2. **Отстраняване на предпоставките за записване на паролите на физически носители.** В голям процент от случаите, поради изисквания свързани с информационната сигурност потребителите трябва да ползват и помнят по няколко различни и сложни пароли, които трябва да бъдат променяни периодично. За да не забравят паролите, служителите ги записват на различни физически носители. Това прави системите несигурни, доколкото различни хора могат да получат достъп до потребителските имена и паролите, а от там и до възможността за осъществяване на нерегламентиран достъп. Чрез възможността за използване на единно потребителско име и парола, заинтересованите лица /лекари и медицински сестри/ могат да запомнят само едно потребителско име и парола, чрез което ще се елиминира този риск за информационната сигурност и ще даде възможност за ползване на една сигурна парола.

3. **Да се осигурят на служителите необходимите им права за достъп.** За да се гарантира сигурността на мрежата и на информационните системи в лечебните заведения, на служителите трябва да се предоставят правилните /необходимите/ права на достъп, въз основа на техните. Осигуряването на предварително определени права на достъп в зависимост от ролята/функцията на потребителя значително подобрява информационната сигурност, като в противен случай следва да бъдат имплементирани допълнителни контроли, което от своя страна би отнело сериозно време и ресурси.

4. **Прилагане на система за управление на достъпите.** Често, когато служители на лечебното заведение напускат работа, IT отделът не е уведомен за това. По този начин потребителския акаунт на потребителят остава активен, което позволява достъп до поверителна информация. Това прави информационните системи в лечебните заведения уязвими, което може да доведе до разгласяване на конфиденциална информация, което от своя страна може да има сериозни последствия. При наличие

на система за управление на достъпите, IT отдела може бързо и лесно да закрива потребителски профили, веднага щом служител напусне, за да се гарантира сигурността на информацията.

5. **Съхраняване на информация за достъпа на потребителите.** Служителите на IT отделът трябва да могат да правят проверки за това коя информация от кой потребител е въведена или коя информация от кого е преглеждана в информационната система.

Все по-широкото използване на информационните технологии в лечебните заведения води до увеличаване възможностите за по-бърз достъп до медицинска информация, но и поставя редица предизвикателства свързани със защитата й. Пациентската информация съдържаща се в болничните информационни системи е чувствителна и строго поверителна, като защитата й е от съществено значение. Нерегламентираният достъп и разгласяването на информация свързана със живота и здравето на пациента може да има етични, социални и правни последици. Именно по тази причина, лечебните заведения трябва да създадат необходимите предпоставки подобряващи начина на работа с информационните системи и информацията съдържаща се в тях, с цел гарантиране на непрекъснатост и високо качество на предоставяните медицински услуги.

Библиография

1. Deshmukh P, Croasdell D. HIPAA: Privacy and security in health care networks. In: Tan J. (editor). Medical informatics: Concepts, methodologies, tools, and applications. New York: IGI Global, 2009: 1897-99
2. Ness R. Influence of the HIPAA privacy rule on health research. J Am Med Assn. 2007; 298(18): 2164-70.
3. Ray A, Newell S. Exploring information security risks in healthcare systems. In: Rodrigues J. (editor). Health information systems: Concepts, methodologies, tools, and applications. New York: IGI Global, 2010: 1716-8
4. Health informatics — Information security management in health using ISO/IEC 27002 (ISO 27799:2008), p.6
5. Ellison, A., Five Ways to Improve Hospital Data Security – Becker's Hospital Review http://www.beckershospitalreview.com/linking-and-reprinting-policy.html