

ПРЕДМЕТ

< ЗДРАВСТВЕНО ИНФОРМАЦИОНИ СИСТЕМИ >

Предавање број 14

**<** **БЕЗБЕДНОСТ ЗДРАВСТВЕНИХ ИНФОРМАЦИОНИХ СИСТЕМА >**

|  |  |  |  |
| --- | --- | --- | --- |
| Недеља | Наставна јединица | Тематске јединице | Резултат – знања или вештине које студент треба да добије |
| 14 | Безбедност здравствених информационих система | Безбедносни програми организација здравствене заштите. Претње информацијама здравствене заштите. | Упознавање са безбедношћу здравствених информационих система. |

Copyright © 2018 – Факултет медицинских наука Универзитета у Крагујевцу. Сва права задржана. Без претходне писмене дозволе од стране Факултета медицинских наука забрањена је репродукција, трансфер, дистрибуција или меморисање неког дела или читавих садржаја овог документа, копирањем, снимањем, електронским путем, скенирањем или на било који други начин.

Copyright © 2018 – Faculty of Medical Sciences of University of Kragujevac. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying,, recording, scanning or otherwise, without the prior written permission of Faculty of Medical Sciences.

**САДРЖАЈ**

[Безбедност здравствених информационих система 2](#_Toc4964720)

[Безбедносни програми организација здравствене заштите 2](#_Toc4964721)

[Претње информацијама здравствене заштите 3](#_Toc4964722)

[Преглед HIPAA безбедносних правила 4](#_Toc4964723)

[Кратак преглед HIPAA безбедносних правила 5](#_Toc4964724)

Предавање бр. 14

**<** **БЕЗБЕДНОСТ ЗДРАВСТВЕНИХ ИНФОРМАЦИОНИХ СИСТЕМА >**

# Безбедност здравствених информационих система

До сада би требало бити јасно да се већина информација у данашњим организацијама здравствене заштите преносе, одржавају и чувају електронски. Електронски медицински записи (ЕМР) системи постају све чешћи, али као што смо видели, чак и информациони системи здравствене заштите засновани на папиру садрже податке и информације које су биле креиране и преношене електронски.

У овом делу дефинишемо сигурност, испитујемо потребу за успостављањем организације-широког безбедносног програма и расправљамо о различитим темама везаним за безбедност. Такође посматрамоа разне постојеће претње информацијама здравствене заштите. Иако се безбедност сигурно заснива на имплементацији HIPAA сигурносних правила, стандарди у овом правилу пружају одлично и сложено сагледавање компоненти неопходних за обезбеђивање здравствених информација и, на неки начин обезбеђују оквир за успостављање одрживог програма безбедносности информација здравствене заштите. Поглавље се затим наставља с погледом на следеће теме, укључујући примере стварних пракси и процедура:

* + Административне заштитне мере
  + Физичке заштитне мере
  + Техничке заштитне мере

Поглавље завршава дискусијом о посебним сигурносним питањима која су повезана са повећаном употребом бежичних мрежа и сродних уређаја у здравственим установама, заједно са дискусијом о сигурносним питањима која се постављају када запослени имају даљински приступ рачунарским мрежама здравствених установа.

## Безбедносни програми организација здравствене заштите

Здравствене установе морају заштитити своје информационе системе од различитих потенцијалних претњи. Међу овим претњама су вируси, пожар у компјутерској соби, непроверени софтвери и крађе клиничких и административних података од стране запослених. Могуће су и претње које укључују намерно или ненамерно оштећење хардвера, софтвера или података или злоупотреба хардвера, софтвера или података здравствене организације.

Реализација било које од ових претњи може проузроковати значајну штету организацији. Прелазак на ручне операције, ако су рачунари у квару у току дана, може довести до хаоса у организацији. Крађа података организације може довести до судских спорова од стране појединаца оштећених откривањем података. Вируси могу покварити базе података, довести до штете и бесповратно уништити податке. Здравствене организације морају имати програме за борбу против кршења безбедности.

Функција безбедносног програма здравствене заштите је да идентификује потенцијалне опасности и спроводе процесе за уклањање ових претњи или ублажавање њихових могућности да изазову штету. На пример, употреба антивирусног софтвера је дизајнирана да смањи претње од вируса; инсталација система противпожарне заштите у рачунарским просторијама је намењена смањењу штете коју може изазвати пожар.

Важно је разумети да је приватност пацијента везана за сигурност. Намерно или ненамерно пуштање информација о пацијентима и њиховим проблемима представља злоупотребу информационих система организације. Безбедност у здравственој организацији, међутим, треба да буде дизајнирана како би се заштитиле не само информације специфичне за пацијенте, већ и за организацију као што су мреже, хардвер, софтвер и апликације које чине информационе системе организација здравствене заштите - од потенцијалних претњи, како претње које долазе од људи тако и од оних које долазе од природних непогода.

Главни изазов развоја ефикасног безбедносног програма у организације здравствене заштите балансира потребу за сигурношћу и трошкове сигурности. Организација не зна како да израчуна вероватноћу да ће хакер изазвати озбиљну штету или да ће ровокопач исећи мрежне каблове испод улице. Организација не може увек разумети у потпуности последице да функционише без мреже током четири сата или четири дана. Стога, није сигурно колико ће потрошити средстава за уклањање или смањење ризика. Ова дилема је слична оној која се поставља када појединци размишљају о дугорочном улагању у осигурање за здравствену заштиту. Нико од нас не зна да ли ће нам требати или нам неће требати ово осигурање, колико дуго ћемо провести у установи за дугорочну негу, или свеобухватност неге која ће нам требати. Колико треба да уложимо у осигурање?

Један аспект овог изазова је одржавање задовољавајуће равнотеже између информације о безбедности здравственог информационог система и здравствене заштите и доступност информација. Као што смо видели, главна сврха одржавања здравствених информација и здравствене евиденције је да олакша квалитетну негу пацијената. С једне стране, ако су мере безбедности организације толико строге да спречавају одговарајући приступ здравственим информацијама потребним за бригу о пацијентима, ова важна сврха је потпкопана. С друге стране, ако организација дозвољава неограничен приступ свим запосленима информацијама везаним за пацијентиме, права пацијената на приватност и поверљивост, сигурно ће бити нарушена и ИТ технологија организације би била под значајним ризиком.

Када здравствене организације развијају своје програме безбедности, требало би да буду сигурне да траже улаз од широког спектра пружаоца здравствених услуга и других корисника система како правних заступника тако и стручњака из области техничких наука. Баланс између приступа и сигурности треба бити такав да заштити права пацијената, а да при томе омогућава одговарајући приступ информацијама.

## Претње информацијама здравствене заштите

Које су претње информационим системима здравствене заштите? Уопште, претње по информациони систем здравствене заштите спадају у једну од ове три категорије:

* + Људске претње, које могу настати услед намерног или ненамерног понашања
  + Природне и еколошке претње, као што су поплаве, пожари и прекид напајања
  + Технички кварови, као што је пад система, а нису сачуване резервне копије

Унутар ових категорија су вишеструке потенцијалне претње. Претње информационим системима здравствене заштите од стране људи могу бити *намерне* или *ненамерне*. Оне могу бити *унутрашње*, узроковане од стране запослених, или *спољашње*, узроковане од стране лица ван организације. Намерне претње укључују крађу, намерну измену података и намерно уништавање података. Кривац би могао бити незадовољан радник, компјутерски хакер, или нешто друго.

У случају Флорида пре неколико година, на пример, кћерка запосленог у болници приступила је поверљивим информацијама преко неадекватне рачунарске радне станице у просторији за хитне случајеве. Написала је имена и адресе недавних пацијената, а потом су позвани да им кажу да су тестирали позитивне на ХИВ. Неколико прималаца ових позива је постало изузетно узрујано.

Компјутерски вируси су међу најчешћим и вирулентним облицима намерног ометања рачунара. Они представљају озбиљну претњу компјутеризованим подацима о пацијенту и здравственој зашити. Неки од узрока ненамерног оштећења информационих система здравствене заштите су недостатак обуке о правилној употреби система или људске грешке. Када корисници деле шифре или преузимају информације са интернет странице која није безбедна, на пример, они стварају потенцијал за нарушавање сигурности.

Унутрашња кршења сигурности су далеко чешћа од екстерних прекршаја. Неки од најчешћих облика унутрашњих кршења безбедности у свим индустријама су инсталирање или коришћење неовлашћеног софтвера, коришћење рачунарских ресурса за незаконите или недозвољене комуникације или активности (порно сурфовање, узнемиравање путем е-маила и тако даље) и употреба рачунарских ресурса за лични профит.

Рачунарски хардвер који се користи у информационим системима здравствене заштите такође мора бити заштићен. Последњих година је било више случајева крађе рачунара из здравствених организација, што доводи до излагања поверљивих информација о пацијенту.

Електронске информације о здравственој заштити су подложне унутрашњим и спољашњим претњама. Било да су намерне или ненамерне, ове претње представљају озбиљне сигурносне ризике. Да би се минимизирао ризик и заштититиле осетљиви информације о пацијенатима, потребне су добро успостављене и имплементиране административне, физичке и техничке сигурносне мере које су суштинске за сваку здравствену установу, без обзира на величину.

Стандарди безбедности успостављени од стране Одељења за здравље и здравствене службе у складу са одредбама Закона о преносивости и одговорности за здравствено осигурање (HIPAA) пружају одличан оквир за развој целокупног плана сигурности и програма за здравствену установу. Прописи су дизајнирани да буду флексибилни и скалабилни и не ослањају се на специфичне технологије за имплементацију, што га чини примењивим за здравствене организације свих величина.

## Преглед HIPAA безбедносних правила

Коначно правило о HIPAA сигурносним стандардима, познато генерално као Правило о безбедности, објављено је у Федералном регистру 20. фебруара 2003. године (68 Фед Фед. 34, 8333-8381). Покривени ентитети (CE) су имале две године да се придржавају правила. Правило безбедности HIPAA је уско повезано са Правилником о приватности. Међутим, док Правило о приватности регулише све заштићене здравствене информације (PHI), Правило сигурности регулише само ePHI. ePHI је дефинисан као заштита здравствених информација које се одржавају или преносе у електронској форми.

Безбедносно правило не прави разлику између електронских облика информација или између преносних механизама. ePHI се може чувати у било ком типу електронских медија, као што су магнетсNE траке и дискови, оптички дискови, сервери и персонални рачунари. Пренос може да потраје постављањем преко Интернета, на локалне мреже (ЛАН) или на дискове, на пример.

Правилник о безбедности HIPAA-а је први пут објављен у августу 1998. Године. Утом тренутку једна од жалби је била да су стандарди превише описни и нису довољно флексибилни. Као резултат, стандарди у коначном правилу су дефинисани у општим условима, фокусирањем о томе шта треба урадити, а не како то треба учинити. Према Центрима за услуге Medicare и Medicaid, коначно правило одређује "серију административних, техничких и физичких сигурносних процедура за покривене ентитете да обезбеди поверљивост електронски заштићених здравствених информација. Стандарди су одређени у захтевима или адресабилним спецификацијама за имплементацију.

Постоји неколико кључних термина које треба дефинисати пре него што испитамо садржај HIPAA-е Безбедносног Правила. Шта је покривени ентитет? Која је разлика између захтеване спецификације имплементације и адресабилности?

Стандарди HIPAA регулишу покривене ентитете (ЦЕ), који су дефинисани као:

* + Здравствени план
  + Клириншка кућа за здравствену заштиту
  + Здравствени радник који преноси заштићене здравствене информације у електронском облику. То практично укључује сваку врсту здравствене организације која се може замислити, укључујући болнице, клинике, ординације лекара, домове за старање и тако даље.

Спецификације садржане у Безбедносном правилу означене су као *обавезне* или *адресабилне*. Потребну спецификацију мора спроводити CE за ту организацију да би била у сагласности. Међутим, CE је у складу са адресабилном спецификацијом ако ради нешто од следећег:

* Спроводи спецификацију како је наведено
* Извршава алтернативну меру сигурности за постизање циљева стандарда или спецификације
* Одлучује да не спроводи ништа, под условом да може доказати да стандард или спецификација није разумна и одговарајућа и да циљеви стандарда и даље могу бити испуњени. Пошто је Правило безбедности дизајнирано да буде технолошки неутрално, ова флексибилност је додељена организацијама које користе не-стандардне технологије или имају легитимне разлоге да не требају наведену спецификацију.

Стандарди садржани у Правилнику о безбедности HIPAA подељени су у пет секција, или категорија. На пример, планови за ванредне ситуације су покривени како административним тако и физичким заштитним мерама и контролом приступа, и обрађени су у неколико стандарда и спецификација. Док читате овај део, размислите како би то функционисало као оквир или модел за програм сигурности организације здравствене заштите.

### Кратак преглед HIPAA безбедносних правила

***Одељак Административних Заштитних секција у коначном правилу садржи девет стандарда:***

1. **Функције управљања сигурношћу**. Овај стандард захтева од ЦЕ да имплементира разне циљеве и процедуре за спречавање, откривање, спречавање и исправљање кршења безбедности.

За овај стандард постоје четири имплементационе спецификације:

■ Анализа ризика (неопходно). ЦЕ мора водити прецизно и темељно процену потенцијалних ризика и рањивости поверљивости, интегритет и доступност еПХИ-а.

■ Управљање ризиком (потребно). ЦЕ мора применити мере безбедности које смањују ризике и рањивост на разумни и одговарајући ниво.

■ Правила санкције (неопходно). ЦЕ мора применити одговарајуће санкције против чланови радне снаге који не испуњавају сигурносна правила ЦЕ ипроцедуре.

■ Ревизија активности информационог система (обавезно). ЦЕ мора подстицати редовно прегледање података о активностима информационог система, као што је ревизија евиденције, извештаји о приступу и извештаји о праћењу инцидента везаних за безбедност.

2. **Додељена безбедносна одговорност**. Овај стандард нема никаквих имплементационих специфичности. Захтева од ЦЕ да идентификује одговорног лица надгледање развоја безбедносних правила и процедура организације.

3.  **Безбедност радне снаге**. Овај стандард захтева да ЦЕ имплементира и да обезбеди да сви чланови радне организације имају одговарајући приступеПХИ и да спречи чланове радне организације који немају дозволу за приступ. За овај стандард постоје три спецификације за имплементацију:

■ Овлашћење и / или надзор (адресабилни). ЦЕ мора имати процес како би осигурали да радна снага која ради са еПХИ има адекватно овлашћење

и надзор.

■ Поступак чишћења радне снаге (адресабилан). Мора постојати процес којим се одређује који приступ је прикладан за сваког члана радне организације.

■ Процедура прекида (адресабилна). Мора постојати процес за прекид приступа еПХИ када члан радне снаге више није запослен или се његове или њене одговорности мењају.

4. **Управљање приступом информацијама**. Овај стандард захтева од ЦЕ да имплементира стандарде и процедуре за одобравање приступа еПХИ-у. Постоје три примене унутар овог стандарда. Први (који није овде приказан) односи се на здравствену заштиту клириншке куће, а друга два се односе на здравствене организације:

■ Овлашћење приступа (адресабилно). ЦЕ мора имати процес дозволе приступа еПХИ преко радне станице, трансакције, програма или другог процеса.

■ Приступ успостављању и модификацији (адресабилни). ЦЕ мора имати право (на основу овлашћења за приступ) да успоставља, документује, прегледа, и измени право корисника на приступ радној станици, трансакцији, програму или процесу.

5. **Свест о сигурности и обуци**. Овај стандард захтева да ЦЕ имплементирапрограме свести и обуке за све чланове своје радне организације. Овај тренингтреба да укључи периодичне сигурносне подсетнике и заштиту адресе од лоших софтвера, надзор над пријављивањем и управљање лозинком. (Ове ствари ће бити део обуке за имплементацију програма.)

6. **Извештавање о безбедносним инцидентима**. Овај стандард захтева да ЦЕ имплементира стандарде и процедуре за решавање сигурносних инцидената.

7. **План ванредног стања**. Овај стандард има пет имплементационих спецификација:

■ План резервне копије података (обавезно).

■ План опоравка од катастрофе (потребан).

■ План рада за хитни режим (потребан).

■ Поступци тестирања и ревизије (адресабилни). ЦЕ треба периодично тестирати

и изменити све планове за ванредне ситуације.

■ Анализа критичности апликација и података (адресабилна). ЦЕ треба да процени

релативна критичност специфичних апликација и података у плану за подршку.

8. **Евалуација.** Овај стандард захтева да ЦЕ периодично обавља техничку и техничку подршку нетехничких оцена као одговор на промене које могу утицати на сигурност еПХИ.

9. **Уговори о пословном удружењу и други аранжмани**. Овај стандард описујеуслове под којима ЦЕ мора имати формални споразум са пословима да би разменили еПХИ.

***Одељак "Физичке заштитне мере" садржи четири стандарда:***

1**. Контрола приступа објекту**. Овај стандард захтева да ЦЕ имплементира стандарде и процедуре за ограничавање физичког приступа његовим електронским информационим системима и објекти у којима су смештени овлашћеним корисницима. Постоје четири примене спецификације са овим стандардом:

■ Операције непредвиђених случајева (адресабилне).

■ План сигурности објекта (адресабилан). ЦЕ мора имати процес за заштиту

објекта и опрему за заштиту од неовлашћеног приступа, уклањања и крађе.

■ Контрола приступа и валидација (адресабилна). ЦЕ треба да има процес

контролу и валидацију приступа објектима на основу улога или функција корисника.

Евиденција о одржавању (адресабилна). ЦЕ треба да има процес документовања

поправке и модификације физичких компоненти објекта као што су они који се односе на сигурност.

2. **Коришћење радне станице**. Овај стандард захтева од ЦЕ да имплементира стандарде и процедуре који одређују одговарајуће функције које треба обавити и на који начин се те функције обављају на одређеној радној станици или класи радних места, а који се може користити за приступ еПХИ-у, и одређује физичке атрибуте околине таквих радних станица.

3. **Безбедност радне станице**. Овај стандард захтева од ЦЕ да имплементира физичко безбедносне страже за све радне станице које се користе за приступ еПХИ-у и за ограничавање приступа овлашћеним корисницима.

4. **Управљачки уређаји и медији**. Овај стандард захтева да ЦЕ имплементира стандарде и процедуре за кретање хардвера и електронских медија који садрже

еПХИ у и из објекта и унутар објекта. Постоје четири имплементације спецификације са овим стандардом:

■ Одлагање (обавезно). ЦЕ мора имати процес за коначну диспозицију еПХИ и хардвера и електронских медија на којима је ускладиштено.

■ Поновна употреба медија (обавезно). ЦЕ мора да има процес уклањања еПХИ-а електронских медија пре него што се медији могу поново користити.

■ Одговорност (адресабилна). ЦЕ мора водити евиденцију покрета хардвера и електронских медија и сваке особе одговорне за ове ставке.

■ Бекап и складиштење података (адресабилно). ЦЕ мора створити обновљиву, тачну копију еПХИ-а, по потреби, пре кретања опреме.

***Одељак Техничких заштитника има пет стандарда:***

1. **Контрола приступа.** Овај стандард захтева да ЦЕ имплементира техничке стандарде и процедуре за електронске информационе системе који одржавају еПХИ како би тако омогућили приступ само лицима или софтверским програмима којима је одобрено право приступа која су наведена у административним заштитним мерама. Постоје четири имплементације спецификације са овим стандардом:

■ Јединствена идентификација корисника (обавезно). ЦЕ мора доделити јединствено име или број за идентификацију и праћење идентитета сваког корисника.

■ Процедура хитног приступа (потребно). ЦЕ мора успоставити процедуре за  
добијање неопходног еПХИ-а у хитним случајевима.  
 ■ Аутоматско одјављивање (адресабилно). ЦЕ мора имплементирати електронске процесекоји прекидају електронску сесију након унапред утврђеног времена неактивности.  
 ■ Шифрирање и дешифровање (адресабилно). ЦЕ треба да примени механизам за шифрирање и дешифровање еПХИ по потреби.

2. **Контрола контроле**. Овај стандард захтева да ЦЕ имплементира хардвер, софтвер, и процедуре које бележе и испитују активности у информационим системима које садрже еПХИ.

3. **Интегритет**. Овај стандард захтева да ЦЕ имплементира правила и процедуре  
заштите еПХИ од неправилне измене или уништења.  
 4. **Аутентичност лица или ентитета**. Овај стандард захтева од ЦЕ да имплементира стандарде да би се потврдило да ли особа или ентитет који тражи приступ еПХИ-у је заправоособаилиентитет.  
 5. **Безбедност преноса**. Овај стандард захтева да ЦЕ имплементира техничку  
подршкукојима се чувају подаци од неовлашћеног приступа еПХИ-у, а који се преносе преко адресабилних мрежа. Постоје две имплементационе спецификације са овим стандардом:  
 ■ Контроле интегритета (адресабилне). ЦЕ мора применити мере безбедности којима се осигурава да електронски преносиви еПХИ није неправилно промењен, али безоткривања.  
 ■ Шифрирање (адресабилно). ЦЕ треба да шифрира еПХИ кад год се сматра то  
прикладним.

***Одељак Правила, Процедуре и Документација има два стандарда:***

1. **Правила и процедуре.** Овај стандард захтева да ЦЕ постави и имплементира  
правила и процедуре за усклађивање са стандардима, специфичности имплементацијеи других захтева.  
 2. **Документација**. Овај стандард захтева од ЦЕ да одржи правила имплементирана у складу са Правилником о сигурности у писменој форми. Постојетри имплементационе спецификације:  
 ■ Временско ограничење (потребно). ЦЕ мора задржати документацију од шест година од датума њеног стварања или датум када је био последњи на снази, у зависности од тога шта је касније.  
 ■ Доступност (потребна). ЦЕ мора доставити документацију и ставити на располагање особама одговорним за спровођење правила и процедура.  
 ■ Ажурирање (обавезно). ЦЕ мора периодично прегледати документацију и  
ажурирати га по потреби.