Розділ 15 Безпека ІС у сфері охорони здоров'я

**Цілі навчання**

* Розуміти важливість створення програми безпеки в масштабах всієї організації охорони здоров'я.
* Вміти ідентифікувати значні загрози - внутрішні, зовнішні, навмисні та ненавмисні - безпеці медичної інформації.
* Вміти окреслити компоненти правил безпеки HIPAA.
* Вміти наводити приклади адміністративних, фізичних та технічних заходів безпеки, що використовуються в даний час в організаціях охорони здоров'я.
* Вміти обговорювати вплив та ризики використання бездротових мереж і надання віддаленого доступу до медичної інформації, а також описувати способи мінімізації ризиків.

Зараз вже має бути зрозуміло, що значна частина інформації в сучасних організаціях охорони здоров'я передається, підтримується і зберігається в електронному вигляді. Системи електронних медичних карток (ЕМК) стають все більш поширеними, але, як ми бачили, навіть переважно паперові інформаційні системи охорони здоров'я містять дані та інформацію, які були створені та передані в електронному вигляді.

У цьому розділі ми даємо визначення безпеки, розглядаємо необхідність створення програми безпеки в масштабах організації та обговорюємо різноманітні теми, пов'язані з безпекою. Ми також розглянемо різні існуючі загрози для медичної інформації. Крім того, ми окреслимо компоненти правил безпеки, передбачених Законом про переносимість і відповідальність за медичне страхування (Health Insurance Portability and Accountability Act, HIPAA). Хоча проблеми безпеки, безумовно, передували впровадженню Правил безпеки HIPAA, стандарти в цьому правилі надають відмінний і всеосяжний опис компонентів, необхідних для захисту медичної інформації, і, до певної міри, забезпечують основу для створення життєздатної програми безпеки медичної інформації. Далі в розділі розглядаються наступні теми, включаючи приклади реальних практик і процедур:

Адміністративні гарантії Фізичні гарантії

Технічні заходи безпеки

Розділ завершується обговоренням особливих питань безпеки, пов'язаних зі зростаючим використанням бездротових мереж і пов'язаних з ними пристроїв в організаціях охорони здоров'я, а також обговоренням питань безпеки, що виникають, коли співробітники мають віддалений доступ до комп'ютерних мереж організацій охорони здоров'я.

*Програма безпеки організації охорони здоров'я*

Організації охорони здоров'я повинні захищати свої інформаційні системи від низки потенційних загроз. Серед цих загроз - віруси, пожежа в комп'ютерній кімнаті, неперевірене програмне забезпечення та крадіжка клінічних і адміністративних даних працівниками. Загрози також можуть включати навмисне або ненавмисне пошкодження обладнання, програмного забезпечення чи даних або неправомірне використання обладнання, програмного забезпечення чи даних організації. Реалізація будь-якої з цих загроз може завдати значної шкоди організації. Звернення до ручної роботи якщо комп'ютери виходять з ладу на кілька днів, це може призвести до організаційного хаосу. Крадіжка організаційних даних може призвести до судових позовів від осіб, які постраждали від розголошення даних. Віруси можуть пошкодити бази даних, після чого відновлення може бути неможливим. Організації охорони здоров'я повинні мати програми для боротьби з порушеннями безпеки.

Функція програми безпеки організації охорони здоров'я полягає у виявленні потенційних загроз і впровадженні процесів, спрямованих на усунення цих загроз або зменшення їхньої здатності завдати шкоди. Наприклад, використання антивірусного програмного забезпечення покликане зменшити загрозу від вірусів; встановлення систем протипожежного захисту в комп'ютерних приміщеннях має на меті зменшити шкоду, яку може завдати пожежа.

Важливо розуміти, як конфіденційність пацієнта пов'язана з безпекою. Навмисне або ненавмисне розголошення інформації, що ідентифікує пацієнта, є неправомірним використанням інформаційних систем організації. Однак безпека в організації охорони здоров'я повинна бути розроблена таким чином, щоб захистити не лише інформацію про пацієнта, але й ІТ-активи організації, такі як мережі, обладнання, програмне забезпечення та додатки, які складають інформаційні системи охорони здоров'я організації, від потенційних загроз, як тих, що походять від людей, так і тих, що походять від природних та екологічних причин.

Основна проблема розробки ефективної програми безпеки в медичній організації полягає в тому, щоб збалансувати потребу в безпеці з витратами на неї. Організація не знає, як розрахувати ймовірність того, що хакер завдасть серйозної шкоди або екскаватор переріже мережеві кабелі під вулицею. Організація може не до кінця розуміти наслідки відсутності мережі протягом чотирьох годин або чотирьох днів. Отже, вона може не бути впевненою, скільки коштів потрібно витратити, щоб усунути або зменшити ризик. Ця дилема подібна до тієї, що постає перед окремими особами, коли вони розглядають можливість отримання страхування на випадок довгострокового догляду. Ніхто з нас не знає, чи знадобиться нам ця страховка, як довго ми можемо прожити в закладі довготривалого догляду, або наскільки гострою буде потреба в догляді. Який обсяг страховки ми повинні придбати?

Одним з аспектів цього виклику є підтримання задовільного балансу між безпекою інформаційної системи охорони здоров'я та доступністю медичних даних та інформації. Як ми бачили в першому розділі, основною метою збереження медичної інформації та медичних записів є сприяння наданню високоякісної медичної допомоги пацієнтам. З одного боку, якщо заходи безпеки організації настільки суворі, що перешкоджають належному доступу до медичної інформації, необхідної для надання допомоги пацієнтам, ця важлива мета підривається. З іншого боку, якщо організація надає необмежений доступ до всієї інформації, що ідентифікує пацієнта, всім своїм працівникам, права пацієнтів на приватність і конфіденційність, безумовно, будуть порушені, а ІТ-активи організації опиняться під значним ризиком.

Розробляючи свої програми безпеки, організації охорони здоров'я повинні обов'язково звертатися до широкого кола постачальників медичних послуг та інших користувачів системи, а також до юрисконсультів і технічних експертів. Баланс між доступом і безпекою має бути розумним - захист прав пацієнтів при забезпеченні належного доступу.

*Загрози для медичної інформації*

Які загрози існують для інформаційних систем охорони здоров'я? Загалом, загрози для інформаційних систем охорони здоров'я відносяться до однієї з цих трьох категорій:

Людські загрози, які можуть виникнути в результаті навмисного або ненавмисного втручання людини

Природні та екологічні загрози, такі як повені, повені та перебої в електропостачанні Технологічні несправності, наприклад, вихід з ладу накопичувача без резервного копіювання

У межах цих категорій існує безліч потенційних загроз. Загрози інформаційним системам охорони здоров'я з боку людей можуть бути навмисними або ненавмисними. Вони можуть бути внутрішніми, спричиненими працівниками, або зовнішніми, спричиненими особами поза межами організації. Навмисні загрози включають крадіжку, навмисну зміну даних і навмисне знищення даних. Винуватцем може бути незадоволений працівник, комп'ютерний хакер або пранкер. Наприклад, кілька років тому у Флориді донька працівника лікарні отримала доступ до конфіденційної інформації через комп'ютерну станцію у відділенні невідкладної допомоги, що залишилася без нагляду. Вона записала імена та адреси нещодавніх пацієнтів, а потім зателефонувала їм і повідомила, що вони отримали позитивний результат тесту на ВІЛ. Декілька одержувачів цих жартівливих дзвінків були вкрай засмучені (Associated Press, 1995a, 1995b).

Комп'ютерні віруси є однією з найпоширеніших і найнебезпечніших форм навмисного втручання в роботу комп'ютера. Вони становлять серйозну загрозу для комп'ютеризованих даних про пацієнтів та медичних програм. (Для отримання додаткової інформації про віруси див. розділ про перевірку на віруси далі в цьому розділі). Деякі з причин ненавмисного пошкодження інформаційних систем охорони здоров'я - недостатня підготовка щодо належного використання системи або людські помилки.

Наприклад, коли користувачі діляться паролями або завантажують інформацію з незахищеного веб-сайту, вони створюють потенціал для порушення безпеки.

Внутрішні порушення безпеки трапляються набагато частіше, ніж зовнішні. Деякі з найпоширеніших форм внутрішніх порушень безпеки в усіх галузях - це встановлення або використання несанкціонованого програмного забезпечення, використання комп'ютерних ресурсів організації для незаконного або протизаконного зв'язку або діяльності (порносерфінг, переслідування електронною поштою тощо), а також використання комп'ютерних ресурсів організації з метою отримання особистої вигоди.

Комп'ютерне обладнання, що використовується в інформаційних системах охорони здоров'я, також має бути захищене від втрати. Останніми роками було зафіксовано багато випадків крадіжок комп'ютерів з організацій охорони здоров'я, що призводило до витоку конфіденційної інформації про пацієнтів (Health Privacy Project, 2007).

Електронна медична інформація вразлива до внутрішніх і зовнішніх загроз. Незалежно від того, навмисні вони чи ненавмисні, ці загрози створюють серйозні ризики для безпеки. Щоб мінімізувати ризик і захистити конфіденційну медичну інформацію пацієнтів, для будь-якої організації охорони здоров'я, незалежно від розміру, необхідні добре розроблені та впроваджені адміністративні, фізичні та технічні заходи безпеки.

Стандарти безпеки, встановлені Міністерством охорони здоров'я і соціальних служб США відповідно до умов Закону про переносимість і підзвітність медичного страхування (HIPAA), забезпечують чудову основу для розробки загального плану і програми безпеки для медичного закладу. Правила розроблені таким чином, щоб бути гнучкими і масштабованими і не залежать від конкретних технологій для впровадження, що дозволяє медичним установам будь-якого розміру відповідати вимогам.

*Огляд Правил безпеки HIPAA*

Остаточне правило щодо стандартів безпеки HIPAA, відоме під загальною назвою "Безпека

Rule, був опублікований у Федеральному реєстрі 20 лютого 2003 року (68 Fed. Reg. 34, 8333-8381). (У третьому розділі ми розглянули різні компоненти далекосяжного законодавства HIPAA. У цьому розділі ми більш детально розглянемо компонент безпеки. Можливо, ви захочете повернутися до третього розділу, щоб дізнатися, як Правило про безпеку вписується в загальний Закон). Покриті суб'єкти (CE) мали два роки на дотримання правил. Правило безпеки HIPAA тісно пов'язане з Правилом конфіденційності HIPAA (також обговорюється в третьому розділі). Однак, якщо Правило про конфіденційність регулює всю захищену медичну інформацію (PHI), то Правило про безпеку регулює лише електронну інформацію про здоров'я (ePHI). EPHI визначається як захищена медична інформація, що зберігається або передається в електронній формі. Правило безпеки не робить різниці між електронними формами інформації або між механізмами передачі. EPHI може зберігатися на будь-яких електронних носіях, таких як магнітні стрічки та диски, оптичні диски, каналізація та персональні комп'ютери. Передача може відбуватися, наприклад, через Інтернет, в локальних мережах (LAN) або на дисках.

Правила безпеки HIPAA були вперше опубліковані у вигляді проекту в серпні 1998 року. На той час однією зі скарг було те, що стандарти були занадто директивними і недостатньо гнучкими. В результаті стандарти в остаточному варіанті визначені в загальних рисах, зосереджуючись на тому, що повинно бути зроблено, а не на тому, як це повинно бути зроблено. За даними Центрів служб Medicare і Medicaid (CMS, 2004), остаточне правило визначає "низку адміністративних, технічних і фізичних процедур безпеки для організацій, які повинні використовуватись для забезпечення конфіденційності електронної захищеної медичної інформації". Стандарти розмежовані на обов'язкові або адресні специфікації впровадження" (див. також Quinsley, 2004; Американська асоціація управління медичною інформацією, 2003a; Gue, 2003).

Перш ніж ми розглянемо зміст Правил безпеки HIPAA, необхідно визначити кілька ключових термінів. Що таке охоплена організація? Яка різниця між обов'язковою специфікацією реалізації та адресною специфікацією?

Стандарти HIPAA регулюють діяльність суб'єктів, що покриваються (CE), які визначаються як Медичний страховий план.

Інформаційний центр з питань охорони здоров'я.

Постачальник медичних послуг, який передає захищену медичну інформацію в електронній формі. Сюди входять практично всі типи медичних організацій, які можна собі уявити, включаючи лікарні, клініки, лікарські кабінети, будинки для людей похилого віку тощо.

Специфікації, що містяться в Правилах безпеки, позначені як обов'язкові або адресні. Обов'язкова специфікація повинна бути реалізована ОЦ для того, щоб організація відповідала вимогам. Однак, ОЦ відповідає адресній специфікації, якщо він виконує будь-яку з наступних дій: Впроваджує специфікацію, як зазначено.

Впроваджує альтернативний захід безпеки для досягнення цілей стандарту або специфікації.

Вирішує не впроваджувати нічого, якщо може продемонструвати, що стандарт або специфікація не є обґрунтованими та доречними, і що мета стандарту все одно може бути досягнута. Оскільки Правило безпеки розроблено таким чином, щоб бути технологічно нейтральним, ця гнучкість була надана організаціям, які використовують нестандартні технології або мають законні причини не потребувати заявленої специфікації (AHIMA, 2003a; Gue, 2003).

Стандарти, що містяться в Правилах безпеки HIPAA, розділені на п'ять розділів, або категорій, специфіку яких ми описуємо тут. Ви помітите, що ці розділи частково перетинаються. Наприклад, плани на випадок надзвичайних ситуацій охоплюються як адміністративними, так і фізичними засобами захисту, а контроль доступу розглядається в декількох стандартах і специфікаціях. У наступних розділах цієї глави ми розглянемо деякі реальні практики, які можуть бути застосовані медичними організаціями в кожній з перших чотирьох категорій. Читаючи цей план, подумайте, як він може працювати в якості основи або моделі для програми безпеки організації охорони здоров'я.

*Короткий виклад правил безпеки HIPAA*

Розділ "Адміністративні гарантії" Заключного регламенту містить дев'ять стандартів:

* Функції управління безпекою. Цей стандарт вимагає, щоб КЕ впроваджував політики та процедури для запобігання, виявлення, стримування та виправлення порушень безпеки.

Існує чотири специфікації реалізації цього стандарту:

* Аналіз ризиків (обов'язковий). КЕ повинен провести точну та ретельну оцінку потенційних ризиків та вразливостей конфіденційності, цілісності та доступності електронної PHI.
* Управління ризиками (обов'язково). КЕ повинен впроваджувати заходи безпеки, які зменшують ризики та вразливості до розумного та належного рівня.
* Політика санкцій (обов'язково). КП повинен застосовувати відповідні санкції до працівників, які не дотримуються політики та процедур безпеки КП.
* Перевірка діяльності інформаційної системи (обов'язкова). КЕ повинен впровадити процедури для регулярного перегляду записів про діяльність інформаційної системи, таких як журнали аудиту, звіти про доступ та звіти про відстеження інцидентів, пов'язаних з безпекою.
* Призначена відповідальність за безпеку. Цей стандарт не має жодних специфікацій щодо впровадження. Він вимагає, щоб КЕ визначив особу, відповідальну за нагляд за розробкою політики та процедур безпеки організації.
* Безпека персоналу. Цей стандарт вимагає, щоб КЗ впроваджував політики та процедури, які гарантують, що всі члени його персоналу мають належний доступ до ePHI, а також запобігають отриманню доступу тими членами персоналу, які не мають такого доступу. Існує три специфікації впровадження цього стандарту: Авторизація та/або нагляд (адресний). КЗ повинен мати процес, який гарантує, що персонал, який працює з електронною персональною інформацією, має відповідні повноваження та нагляд.
* Процедура перевірки персоналу (адресна). Повинен існувати процес для визначення того, який доступ є доречним для кожного працівника.

Процедури припинення (адресні). Повинна існувати процедура припинення доступу до ePHI, коли працівник більше не працює або його обов'язки змінюються.

* Управління доступом до інформації. Цей стандарт вимагає від КЗ впровадження політик та процедур для надання дозволів на доступ до е-ПІП. У цьому стандарті є три специфікації впровадження. Перша (не показана тут) стосується інформаційних центрів охорони здоров'я, а дві інші - організацій охорони здоров'я:
* Авторизація доступу (адресна). ЦО повинен мати процес надання доступу до ePHI через робочу станцію, транзакцію, програму або інший процес. Встановлення та модифікація доступу (адресний). ЦО повинен мати процес (на основі авторизації доступу) для встановлення, документування, перегляду та зміни права користувача на доступ до робочої станції, транзакції, програми або процесу.
* Обізнаність та навчання з питань безпеки. Цей стандарт вимагає, щоб КЕ впроваджував програми підвищення обізнаності та навчання для всіх членів своєї робочої сили. Таке навчання повинно включати періодичні нагадування про безпеку та захист адрес від шкідливого програмного забезпечення, моніторинг входу в систему та управління паролями. (Всі ці питання, які повинні бути розглянуті під час навчання, перераховані як адресні специфікації впровадження).
* Звітування про інциденти безпеки. Цей стандарт вимагає, щоб КЕ впроваджував політику та процедури для реагування на інциденти безпеки.
* План дій у надзвичайних ситуаціях. Цей стандарт має п'ять специфікацій впровадження:
* План резервного копіювання даних (обов'язково). План аварійного відновлення (обов'язково). План роботи в аварійному режимі (обов'язково).

Процедури тестування та перегляду (адресні). КЕ повинен періодично тестувати та змінювати всі плани дій у надзвичайних ситуаціях.

Аналіз критичності додатків та даних (адресний). КЕ повинен оцінити відносну критичність конкретних додатків і даних на підтримку свого плану дій у надзвичайних ситуаціях.

* Оцінювання. Цей стандарт вимагає від ЦОВ періодично проводити технічні та нетехнічні оцінки у відповідь на зміни, які можуть вплинути на безпеку електронної PHI.
* Контракти з діловими партнерами та інші домовленості. Цей стандарт визначає умови, за яких КЕ повинен мати офіційну угоду з діловими партнерами, щоб обмінюватися електронною персональною інформацією.

Розділ "Фізичні гарантії" містить чотири стандарти:

* Контроль доступу до приміщень. Цей стандарт вимагає, щоб КЕ впроваджував політику та процедури для обмеження фізичного доступу до своїх електронних інформаційних систем та приміщень, в яких вони розміщені, лише авторизованими користувачами. Цей стандарт містить чотири специфікації впровадження:
* Операції в надзвичайних ситуаціях (адресні). ЦО повинен мати процедуру надання доступу до об'єкта для підтримки відновлення втрачених даних згідно з планом аварійного відновлення та планом роботи в аварійному режимі.

План забезпечення безпеки об'єкта (адресний). КЕ повинен мати процедуру захисту об'єкта та його обладнання від несанкціонованого доступу, втручання та крадіжки. Контроль та перевірка доступу (з можливістю адресування). КЕ повинен мати процес контролю та перевірки доступу до об'єктів на основі ролей або функцій користувачів.

Записи про технічне обслуговування (адресні). ЦО повинен мати процедуру документування ремонтів та модифікацій фізичних компонентів об'єкта, якщо вони стосуються безпеки.

* Використання робочої станції. Цей стандарт вимагає від КЗ впровадити політики та процедури, які визначають належні функції, що мають виконуватися, та спосіб виконання цих функцій на конкретній робочій станції або класі робочих станцій, які можуть використовуватися для доступу до ePHI, а також визначають фізичні атрибути оточення таких робочих станцій.
* Безпека робочих станцій. Цей стандарт вимагає від ЦО впровадити фізичні засоби захисту для всіх робочих станцій, які використовуються для доступу до ePHI, та обмежити доступ до них лише авторизованими користувачами.
* Контроль пристроїв та носіїв. Цей стандарт вимагає, щоб КЗ впроваджував політику та процедури щодо переміщення обладнання та електронних носіїв, які містять НЗФЛ, на територію та з території закладу, а також у межах закладу. Цей стандарт містить чотири специфікації впровадження:
* Утилізація (обов'язково). КЕ повинен мати процедуру остаточної утилізації еПГЛ, а також апаратного забезпечення та електронних носіїв, на яких вона зберігається.

Повторне використання носія (обов'язково). ЦО повинен мати процедуру видалення ePHI з електронних носіїв перед тим, як носій може бути використаний повторно.

Підзвітність (адресна). КЕ повинен вести облік переміщення апаратних засобів та електронних носіїв і всіх осіб, відповідальних за ці предмети. Резервне копіювання та зберігання даних (з можливістю адресації). За необхідності, перед переміщенням обладнання, КЕ повинна створити доступну, точну копію електронної персональної інформації, яку можна відновити.

Розділ "Технічні гарантії" складається з п'яти стандартів:

* Контроль доступу. Цей стандарт вимагає від КЕ впровадження технічних політик і процедур для електронних інформаційних систем, які зберігають ePHI, щоб дозволити доступ тільки тим особам або програмам, яким надані права доступу, як зазначено в адміністративних гарантіях. Цей стандарт містить чотири специфікації впровадження:
* Унікальна ідентифікація користувача (обов'язкова). КЕ повинен присвоїти унікальне ім'я або номер для ідентифікації та відстеження особи кожного користувача.

Процедура екстреного доступу (обов'язкова). КЕ повинен встановити процедури для отримання необхідної ePHI в екстрених випадках.

Автоматична реєстрація (адресна). КЕ повинен впровадити електронні процеси, які припиняють електронну сесію після заздалегідь визначеного часу бездіяльності. Шифрування та дешифрування (адресне). КЕ повинен впровадити механізм шифрування та дешифрування еПДП за потреби.

* Аудиторський контроль. Цей стандарт вимагає, щоб КЕ впровадив апаратне, програмне забезпечення та процедури, які реєструють та перевіряють діяльність в інформаційних системах, що містять еПНП.
* Цілісність. Цей стандарт вимагає, щоб КЕ впроваджував політики та процедури для захисту ePHI від неналежної зміни або знищення.
* Аутентифікація особи або організації. Цей стандарт вимагає, щоб КЕ впровадив процедури для перевірки того, що особа або організація, яка бажає отримати доступ до електронної персональної інформації, дійсно є тією особою або організацією, за яку вона себе видає.
* Безпека передачі. Цей стандарт вимагає від КЕ впровадження технічних заходів для захисту від несанкціонованого доступу до ePHI, що передається мережею. Існує дві специфікації впровадження цього стандарту:
* Контроль цілісності (адресний). ЦО повинен впроваджувати заходи безпеки, щоб гарантувати, що передана в електронному вигляді ePHI не буде неналежним чином модифікована без виявлення. Шифрування (адресне). КЕ повинен шифрувати електронну PHI, коли це вважається доцільним.

Розділ "Політика, процедури та документація" має два стандарти:

* Політики та процедури. Цей стандарт вимагає, щоб КЕ розробив та впровадив політику та процедури для дотримання стандартів, специфікацій впровадження та інших вимог.
* Документація. Цей стандарт вимагає, щоб КЕ підтримував політику та процедури, впроваджені для дотримання Правил безпеки, у письмовій формі. Існує три специфікації впровадження:

Термін зберігання (обов'язково). КЕ повинен зберігати документацію протягом шести років з дати її створення або з дати, коли вона востаннє діяла, залежно від того, яка з цих дат є пізнішою.

Доступність (обов'язково). КЕ повинен зробити документацію доступною для осіб, відповідальних за впровадження політик та процедур.

Оновлення (обов'язкові). КЕ повинен періодично переглядати документацію та оновлювати її за необхідності.

У цьому розділі наведено огляд ключових компонентів стандартів безпеки HIPAA (68 Fed. Reg. 34, 8333-8381, 20 лютого 2003 р.). У наступних розділах ми розглянемо деякі практики, які можуть бути використані для дотримання правил і забезпечення ефективної програми безпеки в організації.

*Адміністративні гарантії*

Як ви бачили з огляду стандартів HIPAA, адміністративні гарантії охоплюють широкий спектр організаційних заходів. У цьому розділі ми не намагаємося дати всебічний, детальний огляд усіх можливих адміністративних заходів захисту, а скоріше представити кілька практик, які можна використовувати як частину загальних адміністративних зусиль, спрямованих на покращення програми інформаційної безпеки організації охорони здоров'я. Ми обговоримо наступні теми: Аналіз та управління ризиками Керівник служби безпеки Оцінка безпеки системи

Аналіз та управління ризиками

Одним із ключових компонентів застосування адміністративних гарантій для захисту медичної інформації організації є аналіз ризиків. Неможливо створити ефективну програму управління ризиками, якщо організація не знає про існуючі ризики чи загрози. Аналіз ризиків є відносно новим явищем у сфері охорони здоров'я. Лише деякі організації впровадили формальну оцінку ризиків безпеки до публікації правил HIPAA. Це жодним чином не применшує її важливості. Однак, за прикладами процесів оцінки ризиків охороні здоров'я доводилося звертатися до інших галузей (Walsh, 2003; Reynolds, 2009).

Стів Вейл (2004) на веб-сайті HIPAAdvisory.com визначає ризик як

"ймовірність того, що конкретна загроза використає певну вразливість, і наслідки цієї події". Він представляє процес аналізу ризиків, що складається з восьми частин, або кроків:

* *Визначення меж*. На етапі визначення меж організація повинна розробити детальний перелік всієї медичної інформації та інформаційних систем. Цей огляд можна провести за допомогою інтерв'ю, перевірок, анкетування або інших засобів. На цьому етапі важливо визначити всю медичну інформацію про пацієнта, інформаційні системи охорони здоров'я (як внутрішні, так і зовнішні), а також користувачів цієї інформації та систем.
* *Ідентифікація загроз*. В результаті ідентифікації загроз буде складено перелік усіх потенційних загроз для інформаційних систем охорони здоров'я організації. Три основні типи загроз, які слід враховувати: a. Природні, такі як повені та пожежі
* Людська, яка може бути навмисною або ненавмисною
* Екологічні, такі як перебої в електропостачанні
* *Ідентифікація вразливостей*. На цьому етапі організація визначає всі конкретні вразливості, які існують у її власних інформаційних системах охорони здоров'я. Як правило, вразливості проявляються у вигляді недоліків або слабких місць у процедурах або дизайні системи. Існують програмні пакети, які допомагають у виявленні вразливостей, але організації також може знадобитися проведення інтерв'ю, опитувань тощо. Деякі організації можуть залучати зовнішніх консультантів для виявлення вразливостей у своїх системах.
* *Аналіз засобів контролю безпеки*. Організація також повинна провести ретельний аналіз наявних засобів контролю безпеки. До них відносяться як превентивні засоби контролю, такі як контроль доступу та процедури автентифікації, так і засоби контролю, призначені для виявлення фактичних або потенційних порушень, такі як аудиторські сліди та тривоги.
* *Визначення ймовірності ризику*. На цьому етапі процесу кожній області інформаційної системи охорони здоров'я присвоюється рейтинг ризику. Існує безліч рейтингових систем, які можуть бути використані. Weil рекомендує використовувати досить просту систему оцінювання високого, середнього та низького ризиків.
* *Аналіз впливу*. Це етап, на якому організація визначає, яким буде фактичний вплив конкретних порушень безпеки. Порушення може вплинути на конфіденційність, цілісність або доступність. Вплив також може бути оцінений як високий, середній або низький.
* *Визначення ризику*. Інформація, зібрана до цього моменту в процесі аналізу ризиків, зводиться воєдино для того, щоб визначити фактичний рівень ризику для конкретної інформації та конкретних інформаційних систем. Визначення ризику ґрунтується на
* Ймовірність того, що певна загроза спробує використати певну вразливість (висока, середня або низька)
* Рівень впливу, якщо загроза успішно скористається вразливістю

(високий, середній або низький)

* Адекватність запланованих або існуючих засобів контролю безпеки (висока, середня або низька) Кожна конкретна система або тип інформації може бути оцінена за кожним з цих трьох факторів, а потім ці оцінки можуть бути об'єднані для отримання загального рейтингу ризику: високий - потребує негайної уваги, середній - потребує уваги найближчим часом, або низький - існуючі засоби контролю є прийнятними.
* *Рекомендації щодо контролю безпеки*. Заключним етапом процесу є складання зведеного звіту за результатами аналізу та рекомендацій щодо вдосконалення засобів контролю безпеки.

Аналіз ризиків повинен призвести до розробки політики та процедур, що визначають процедури управління ризиками, а також санкції або наслідки для працівників та інших осіб, які не дотримуються встановлених процедур. Всі організації охорони здоров'я повинні мати офіційну програму управління ризиками безпеки. Як правило, цією програмою керує співробітник служби безпеки організації.

Начальник служби безпеки

Кожна організація охорони здоров'я повинна мати єдину особу, яка відповідає за нагляд за програмою інформаційної безпеки. Як правило, ця особа призначається керівником служби безпеки організації. Керівник служби безпеки може підпорядковуватися директору з інформаційних технологій (ІТ-директору) або іншому адміністратору в організації охорони здоров'я. Роль особи, відповідальної за безпеку, може становити 100 відсотків посадових обов'язків особи або лише частину, залежно від розміру організації та обсягу її інформаційних систем охорони здоров'я. Незалежно від фактичної структури підпорядкування, важливо, щоб керівник служби безпеки був наділений повноваженнями для ефективного управління програмою безпеки, застосування санкцій та впливу на співробітників. Як зазначив Том Волш (2003, с. 15), визначаючи важливість посади керівника служби безпеки, "вплив може залучити потрібних людей до виконання роботи".

Оцінка безпеки системи

Керівники служби безпеки повинні періодично оцінювати інформаційні системи та мережі охорони здоров'я своєї організації на предмет належного технічного контролю та процесів. Очевидно, що встановлений набір технічних стандартів безпеки медичної інформації полегшив би цей процес оцінювання. На жаль, наразі не існує загальноприйнятих стандартів технічної безпеки, розроблених для інформаційних систем охорони здоров'я (нагадаємо, що стандарти HIPAA є технологічно нейтральними). Однак існують загальні стандарти для методів безпеки для всіх типів організацій, які були розроблені Міжнародною організацією зі стандартизації (ISO), як стандарт ISO

15408 (під назвою "Інформаційні технології - Методи безпеки - Критерії оцінки безпеки ІТ"). Ці стандарти, оновлені в 2005 році, дозволяють організаціям використовувати загальний набір вимог і, таким чином, порівнювати результати незалежних оцінок безпеки (ISO, 2005).

*Фізичний захист*

Програма безпеки повинна передбачати фізичні, а також технічні та адміністративні засоби захисту. Фізичні заходи безпеки передбачають захист власне комп'ютерного обладнання, програмного забезпечення, даних та інформації від фізичного пошкодження або втрати через природні, людські або екологічні загрози. У цьому розділі розглядаються деякі конкретні питання, пов'язані з фізичною безпекою. Розподіл відповідальності за безпеку

* Керування мультимедіа
* Контроль фізичного доступу
* Безпека робочих станцій
* Призначена відповідальність за безпеку

Кожен компонент інформаційної системи охорони здоров'я має бути захищеним, і за його безпеку має відповідати один працівник, якого легко ідентифікувати. Ці особи, в свою чергу, підзвітні керівнику служби безпеки. Наприклад, у відділенні медсестер керівник відділення може відповідати за те, щоб усі працівники були навчені розуміти та застосовувати заходи безпеки, а також усвідомлювали важливість підтримки безпеки інформації про пацієнтів. Мережевий адміністратор, однак, може бути особою, відповідальною за призначення початкових паролів і закриття доступу працівникам, які звільняються або переводяться до інших відділень (Рейнольдс, 2009).

Керування засобами масової інформації

Фізичні носії, на яких зберігається медична інформація, повинні бути фізично захищені. Контроль за носіями інформації - це політика та процедури, які регулюють отримання та вилучення апаратного, програмного забезпечення та комп'ютерних носіїв, таких як диски та стрічки, а також їхнє переміщення в організації та за її межами.

Контроль за носіями також охоплює зберігання даних. Наприклад, касети з резервними копіями повинні зберігатися в безпечному місці з обмеженим доступом. Остаточна утилізація електронних носіїв є ще одним аспектом контролю за носіями інформації. Політика знищення інформації про пацієнтів повинна стосуватися електронних носіїв та обладнання (робочих станцій і серверів), які містять інформацію про пацієнтів. Коли організації збирають старі комп'ютери, всі дані пацієнтів мають бути видалені до того, як це обладнання стане надлишковим або буде утилізоване в інший спосіб (Reynolds, 2009).

Контроль фізичного доступу

Засоби контролю фізичного доступу призначені для обмеження фізичного доступу до медичної інформації особами, які мають на це право. Замки та ключі є прикладами фізичного контролю доступу. Однак, очевидно, що всі робочі місця не можна тримати під замком. Це може створити безпечну систему, але вона не буде легкодоступною для медичних працівників, яким потрібна інформація про пацієнта. Деякі з компонентів контролю фізичного доступу, які можуть бути застосовані, - це контроль обладнання; план безпеки закладу; процедури, які перевіряють особу користувача перед тим, як надати йому фізичний доступ до певної зони; процедура ведення обліку ремонтів та модифікацій обладнання, програмного забезпечення та фізичного обладнання; процедура реєстрації відвідувачів. Організації повинні мати систему, наприклад, систему інвентаризації, яка точно визначає, яке обладнання використовується в їхній інформаційній системі охорони здоров'я в даний момент. Система інвентаризації, як правило, передбачає маркування або позначення кожної одиниці обладнання унікальним номером, а також закріплення кожної одиниці за певним місцем і відповідальною особою. Коли обладнання переміщується, списується або знищується, ця дія має бути задокументована в системі управління запасами. Іншою формою контролю обладнання є встановлення протикрадіжних пристроїв, таких як ланцюги, що прикріплюють комп'ютери до столів, сигналізація та інші засоби, що відлякують злодіїв.

План безпеки закладу - це план, який гарантує, що особи, які перебувають у певній зоні, мають дозвіл на доступ до цієї зони. Основні комп'ютерні операції організації охорони здоров'я, як правило, знаходяться під суворим контролем, включаючи відеоспостереження та перевірки особистої безпеки. У закладах охорони здоров'я поширені бейджі з фотографіями, які допомагають ідентифікувати персонал, що має право доступу до певних будівель та приміщень. У деяких охоронюваних зонах для входу потрібно ввести код на клавіатурі або провести ідентифікаційною карткою по зчитувачу, щоб отримати дозвіл на вхід. План безпеки об'єкта також повинен містити процедури допуску відвідувачів. Наприклад, кожен відвідувач може зареєструватися та отримати тимчасову ідентифікаційну перепустку. В організації можуть бути зони, які взагалі не відкриті для відвідувачів (Рейнольдс, 2009).

Безпека робочих станцій

Робочі місця, які надають доступ до інформації про пацієнта, повинні бути розміщені в місцях, які є безпечними або перебувають під постійним наглядом. Робочі місця в приймальні або інших громадських місцях повинні бути розташовані таким чином, щоб відвідувачі або інші особи не могли бачити екран. Над моніторами робочих станцій можна розмістити пристрої, які не дозволять людям читати екран, якщо вони не перебувають безпосередньо перед ним. Ще одним аспектом безпеки робочих місць є розробка чітких правил користування ними. Ці політики повинні визначати, серед іншого, відповідні функції, які слід виконувати на робочій станції, та правила спільного використання робочих станцій.

Організації, які дозволяють працівникам працювати з дому, стикаються з додатковими проблемами безпеки робочих місць. Працівники, які працюють вдома, повинні отримати чіткі інструкції щодо належного використання комп'ютерних ресурсів організації, незалежно від того, чи стосуються ці ресурси апаратного, програмного забезпечення або доступу до Інтернету. Працівники повинні отримувати доступ до будь-якої інформації, що може ідентифікувати пацієнта, через захищене з'єднання, з належним моніторингом, щоб переконатися, що користувач дійсно є уповноваженим працівником.

Всі аспекти фізичної безпеки вимагають належного навчання всього персоналу, який має потенційний доступ до інформаційних систем охорони здоров'я. Працівники, агенти та підрядники, які мають доступ до місць, де зберігається інформація про пацієнтів, повинні брати участь у навчанні з питань безпеки та конфіденційності (Reynolds, 2009).

*Технічні заходи безпеки*

Для захисту інформаційних систем охорони здоров'я та мереж, в яких вони розміщені, можна використовувати багато різних технічних засобів захисту. Знову ж таки, ми не надамо вичерпного переліку всіх доступних засобів захисту, але наведемо кілька репрезентативних прикладів. Ми обговоримо технічні засоби захисту, пов'язані з наступними темами: Контроль доступу Аутентифікація суб'єкта Аудиторські записи Шифрування даних Захист брандмауером Перевірка на віруси

Контроль доступу

Доступ до медичної інформації, що ідентифікує особу пацієнта, повинні мати лише особи, яким це необхідно. Сучасні комп'ютерні системи, включаючи бази даних і мережі, дозволяють користувачам отримувати доступ до різноманітних ресурсів, таких як окремі файли, файли баз даних і стрічки, а також використовувати принтери та інші периферійні пристрої. Таке спільне використання ресурсів є важливим компонентом ефективних інформаційних систем охорони здоров'я, але воно вимагає, щоб адміністратори мережі та адміністратори баз даних встановлювали відповідні права доступу для кожного ресурсу. Часто користувачам медичної інформаційної системи доводиться призначати права доступу до мережі та окремі права доступу до додатків, перш ніж вони зможуть користуватися системою.

Контроль за доступом до медичних даних може включати будь-який з наступних методів:

Доступ на основі користувачів Доступ на основі ролей

Контекстний доступ

Перш ніж ми обговоримо кожен з цих варіантів, необхідно коротко пояснити, що таке права доступу. Традиційні права доступу на основі користувачів і ролей мають два параметри - хто і як. Хто - це список користувачів, які мають право доступу до інформації або комп'ютерного ресурсу, про який йде мова. Цей список, який називається списком контролю доступу, може бути організований за окремими користувачами або за групами користувачів. Ці групи зазвичай визначаються за роллю або робочою функцією. Наприклад, усі кодувальники у відділі управління медичною інформацією матимуть однакові права доступу, усі зареєстровані медичні сестри певної кваліфікації матимуть однаковий доступ тощо.

Параметр how схеми контролю доступу визначає, як користувач може отримати доступ до ресурсу. Типові дії, які можуть бути дозволені користувачам: читання, запис, редагування, виконання, додавання та друк. Тільки так званим власникам і адміністраторам будуть надані повні права, щоб вони могли змінювати, видаляти або створювати нові компоненти ресурсу. Очевидно, що привілеї власників та адміністраторів на використання інформаційних систем охорони здоров'я повинні ретельно контролюватися.

***Контроль доступу на основі користувачів*** визначається як "механізм безпеки, що використовується для надання користувачам доступу до системи на основі ідентифікації користувача". При контролі доступу на основі ролей (RBAC) рішення про доступ приймаються на основі ролей, які виконують окремі користувачі в організації. "За допомогою RBAC, замість того, щоб намагатися зіставити політику безпеки організації з відносно низькорівневим набором технічних засобів контролю (як правило, списками контролю доступу), кожному користувачеві призначається одна або декілька заздалегідь визначених ролей, кожній з яких надаються різні привілеї, необхідні для виконання ролі" (63 Fed. Reg. 155, 12 серпня 1998 р.). Однією з переваг доступу на основі ролей над доступом на основі користувачів є те, що в міру додавання нових додатків привілеї легше призначати. Дискреційне призначення доступу адміністратором обмежене за допомогою RBAC. Користувачі повинні бути призначені до певної ролі, щоб отримати доступ до певної програми.

***Контроль доступу на основі контексту*** є найсуворішим з трьох варіантів. Гаррі Сміт (2001) описує його таким чином: "Контекстно-орієнтована схема контролю доступу починається із захисту, що забезпечується або користувацьким, або рольовим контролем доступу, і робить ще один крок вперед ..... Контекстно-орієнтований контроль доступу враховує особу, яка намагається отримати доступ до даних, тип даних, до яких здійснюється доступ, і контекст транзакції, під час якої здійснюється спроба доступу". Іншими словами, контекстно-орієнтований доступ враховує три параметри - хто, як і контекст, в якому здійснюється доступ до даних. Наступний приклад ілюструє відмінності між цими трьома типами контролю доступу (Рейнольдс, 2009).

Автентифікація суб'єкта

Механізми контролю доступу є ефективним засобом контролю за тим, хто отримує доступ до інформаційної системи охорони здоров'я, лише тоді, коли існує система забезпечення ідентифікації особи, яка намагається отримати доступ. Автентифікація суб'єкта визначається в Правилах безпеки HIPAA як "підтвердження того, що особа є саме тією, за яку себе видає". Автентифікація суб'єкта, пов'язана з інформаційними системами охорони здоров'я, повинна включати щонайменше (1) автоматичний вихід з системи та (2) унікальний ідентифікатор користувача (Reynolds, 2009).

Автоматичний вихід з системи - це процедура безпеки, яка призводить до завершення сеансу роботи з комп'ютером після заздалегідь визначеного періоду бездіяльності, наприклад, через десять хвилин. Існує багато програмних продуктів, які дозволяють мережевим адміністраторам встановлювати параметри автоматичного виходу з системи. Після встановлення ці системи виходу з системи діють як звичайна заставка на звичайній робочій станції, яка вмикається після певного періоду бездіяльності. Після цього користувачі повинні ввести мережевий пароль, щоб деактивувати екран системи автоматичного завершення роботи. Як правило, також встановлюється драйвер пристрою, який запобігає перезавантаженню для деактивації системи виходу з системи. Інші заходи безпеки, які можуть бути включені в продукти з автоматичним виходом з системи, - це функції, які не дозволяють користувачам змінювати заставку і дозволяють уповноваженій особі встановлювати локальні паролі на випадок, якщо користувач не підключений до мережі. Невдалі спроби входу в систему можуть реєструватися та відображатися у звітах разом зі статистикою входів користувачів, часу, що минув, та ідентифікації користувачів.

Кожному користувачеві медичної інформаційної системи має бути присвоєно унікальний ідентифікатор. Цей ідентифікатор - це комбінація символів і цифр, яку призначає і підтримує система безпеки. Він використовується для відстеження індивідуальної активності користувача. Цей ідентифікатор зазвичай називають ідентифікатором користувача або ідентифікатором входу в систему. Це загальнодоступна, або відома, частина більшості процедур входу в систему. Наприклад, багато організацій призначають ідентифікатор для входу в систему, який збігається з адресою електронної пошти користувача або комбінацією прізвища та імені користувача. Як правило, досить легко ідентифікувати користувача за його ідентифікатором. Наприклад, ідентифікатор користувача John Doe може бути "doej". Через публічний характер входу в систему потрібні додаткові засоби захисту, окрім ідентифікатора входу в систему.

Автентифікація суб'єкта може бути реалізована в інформаційній системі охорони здоров'я кількома різними способами. Найпоширенішим методом автентифікації суб'єкта є система паролів. Інші механізми включають персональні ідентифікаційні номери (PIN-коди), системи біометричної ідентифікації, системи телефонних дзвінків і токени. Ці методи можуть використовуватися окремо або в поєднанні з іншими системами. Експерти з безпеки часто заохочують багаторівневі системи безпеки, які використовують більше одного механізму захисту. Як сказав один експерт з безпеки: "Серія рішень, що перекривають один одного, працює набагато ефективніше, навіть якщо ви знаєте, що кожне з них окремо є помилковим. Якщо ви вишикуєте три засоби захисту, кожен з яких ефективний на 60 відсотків, то разом вони будуть ефективні на 90 відсотків проти певної атаки" (Briney, 2000).

Волш (2003) рекомендує систему, яка використовує двофакторну автентифікацію. Він виділяє ці три методи автентифікації, і будь-які два з них, що використовуються разом, є двофакторною системою:

Щось, що ви знаєте, наприклад, пароль або персональний ідентифікаційний номер (PIN-код) Щось, що у вас є, наприклад, картка банкомату, токен або свайп-картка.

Щось, чим ви є, наприклад, біометричний відбиток пальця, сканування голосу або сканування райдужної оболонки ока чи сітківки [Walsh, 2003].

**Системи паролів** Найпоширенішим способом контролю доступу до інформаційної системи охорони здоров'я (або будь-якої іншої комп'ютерної системи) є комбінація ідентифікатора користувача та пароля або PIN-коду. Ідентифікатори користувачів та паролі для системи зберігаються або як частина списку контролю доступу для мережевої чи локальної операційної системи, або в спеціальній базі даних. Потім здійснюється пошук збігу в списку або базі даних, перш ніж користувачеві буде дозволено отримати доступ до системи, до якої він звернувся. Хоча ідентифікатор користувача не є таємницею, пароль або PIN-код є таємницею. Паролі зазвичай зберігаються в зашифрованому вигляді, який неможливо розшифрувати (White, 2001; Oz, 2006).

Хоча системи паролів та PIN-кодів є найпоширенішими формами автентифікації суб'єктів, вони також забезпечують найслабшу форму безпеки. За визначенням Whatis?.com (2002), пароль - це "послідовність символів без пробілів, яка використовується для визначення того, що користувач комп'ютера, який запитує доступ до комп'ютерної системи, є саме цим користувачем". Зазвичай пароль складається з чотирьох-шістнадцяти символів. Однією з найбільших проблем з паролями є те, що користувачі можуть ділитися ними або публічно демонструвати їх. Користувачі часто записують паролі, які не можуть запам'ятати. Вони можуть навіть записати пароль на магнітну стрічку або розмістити його на робочій станції комп'ютера. Організації охорони здоров'я повинні вжити заходів, щоб запобігти такому типу зловживань паролями. Важливими є чітка політика щодо використання та збереження паролів, навчання працівників та дієві санкції для порушників політики.

Ще одна поширена проблема з паролями полягає в тому, що якщо вони досить прості для запам'ятовування, то можуть бути досить простими для того, щоб їх міг вгадати хтось інший. Паролі шифруються, але існують програми, так звані "зломщики паролів", які можна використовувати для визначення невідомого або забутого пароля. На жаль, неавторизовані особи, які прагнуть отримати доступ до комп'ютерних систем, також можуть використовувати ці програми (White, 2001; Whatis?.com, 2002). Організації охорони здоров'я повинні встановити чіткі рекомендації щодо вибору паролів, які підлягають виконанню. У наступному огляді наведено деякі пропозиції (White, 2001; Whatis?.com, 2002; Reynolds, 2009).

|  |
| --- |
| **ПАРОЛЬ МОЖНА І НЕ МОЖНА**  НЕ МОЖНА  Виберіть пароль, який легко вгадає той, хто вас знає (наприклад, не використовуйте свій номер соціального страхування, дату народження, дівоче прізвище, ім'я домашнього улюбленця, ім'я дитини або назву автомобіля).  Виберіть слово, яке можна знайти у словнику (тому що програми-зломщики можуть швидко спробувати кожне слово зі словника!).  Виберіть слово, яке наразі є новинним. Виберіть пароль, схожий на ваш попередній пароль.  Поділіться своїм паролем з іншими.    МОЖНА  Виберіть комбінацію букв і принаймні однієї цифри. Виберіть пароль щонайменше з восьми символів, змішуючи великі та малі літери, якщо ваша система паролів чутлива до регістру.  Виберіть слово, яке ви легко запам'ятаєте.  Часто змінюйте свій пароль. (Деякі мережі вимагають періодичної зміни пароля). |

**Біометричні системи ідентифікації** Через недоліки, притаманні системам паролів, були розроблені інші системи ідентифікації. Біометричні системи ідентифікації використовують біологічні дані користувачів у вигляді, наприклад, відбитка голосу, відбитків пальців, відбитків рук, сканування сітківки ока, відбитків обличчя або повного сканування тіла. Хоча деякі джерела (White, 2001) називають системи біометричної ідентифікації "хвилею майбутнього", є ознаки того, що ця технологія ще не набула широкого застосування.

Тим не менш, біометрія, ймовірно, буде відігравати все більшу роль у забезпеченні безпеки інформаційних систем охорони здоров'я. Біометричні пристрої складаються зі зчитувального або скануючого пристрою, програмного забезпечення, яке перетворює відскановану інформацію в цифрову форму, і бази даних, яка зберігає біометричні дані для порівняння. IBM, Microsoft, Novell та інші комп'ютерні компанії зараз працюють над стандартом для біометричних пристроїв під назвою BioAPI. Цей стандарт дозволить програмним продуктам різних виробників взаємодіяти один з одним (Whatis?.com, 2002).

**Процедури зворотного телефонного дзвінка** Процедури зворотного телефонного дзвінка є ще однією формою автентифікації суб'єкта, яка використовується сьогодні. Зворотній дзвінок використовується переважно тоді, коли працівники мають доступ до інформаційної системи охорони здоров'я з дому. Коли модем підключається до системи, спеціальна програма для зворотного дзвінка запитує номер телефону, з якого було здійснено дзвінок. Якщо цей номер не є авторизованим, програма зворотного дзвінка не дозволить доступ (Oz, 2004).

**Токени** Токени - це пристрої, такі як картки-ключі, які вставляються в двері або комп'ютери. У системах автентифікації за допомогою токенів ідентифікація ґрунтується на володінні користувачем токеном (Eng, 2001). Недоліком токенів є те, що вони можуть бути втрачені, загублені або вкрадені. Коли токени використовуються в поєднанні з паролем або PIN-кодом, важливо, щоб пароль або PIN-код не були записані на токені або в місці, де він зберігається.

Аудиторські сліди

Webopedia.com (2004:1) визначає аудиторський слід як "запис, що показує, хто мав доступ до комп'ютерної системи і які операції він або вона виконували протягом певного періоду часу. Крім того, існують окремі програмні продукти, що дозволяють мережевим адміністраторам контролювати використання мережевих ресурсів". Аудиторські сліди генеруються спеціалізованим програмним забезпеченням і мають безліч застосувань у захисті інформаційних систем. Ці застосування можна класифікувати наступним чином (Gopalakrishna, 2000):

Індивідуальна підзвітність. Коли дії працівників або інших осіб відстежуються за допомогою аудиторського сліду, ці особи стають підзвітними за свої дії, що може бути сильним стримуючим фактором для порушення прийнятних політик і процедур. Реконструкція електронних подій. Аудиторські сліди також можна використовувати для реконструкції того, як і коли використовувався комп'ютер або програма. Це може бути дуже корисно, коли є підозра на порушення безпеки, як внутрішнє, так і зовнішнє.

Моніторинг проблем. Деякі типи програмного забезпечення для аудиту можуть виявляти такі проблеми, як збій диска, надмірне використання системних ресурсів і перебої в роботі мережі в міру їх виникнення.

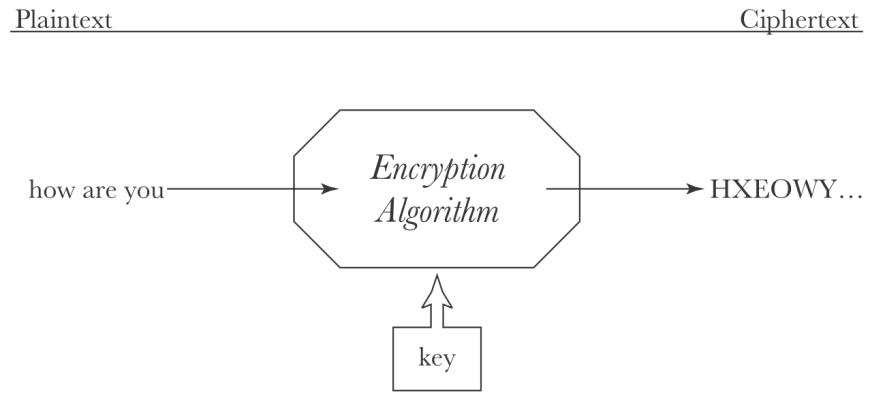
Виявлення вторгнень. Коли є спроби отримати несанкціонований доступ до системи, система аудиту може їх виявити.

Шифрування даних

Шифрування даних використовується для того, щоб гарантувати, що дані, які передаються з одного місця в мережі в інше, захищені від підслуховування або перехоплення. Це стає особливо важливим, коли конфіденційні дані, такі як медична інформація, передаються через загальнодоступні мережі, такі як Інтернет, або через бездротові мережі. Безпечні дані - це дані, які неможливо перехопити, скопіювати, змінити або видалити як під час передачі, так і під час зберігання, наприклад, на диску чи стрічці.

Криптографія вивчає методи шифрування та дешифрування. Це складна наука з великою кількістю пов'язаних з нею методів. У цій главі будуть розглянуті лише основні поняття та деякі сучасні технології автентифікації. Інфраструктура відкритих ключів, Pretty Good Privacy, дротовий еквівалент конфіденційності (WEP) і захищений доступ до Wi-Fi (WPA) - це форми шифрування, які сьогодні використовуються в організаціях охорони здоров'я. (WEP і WPA застосовуються саме до бездротових мереж і будуть розглянуті далі в цьому розділі). Ці протоколи використовуються для автентифікації відправників і одержувачів повідомлень, що передаються через публічні мережі, такі як Інтернет або бездротові мережі.

Деякі основні терміни, пов'язані з шифруванням, - це відкритий текст, алгоритм шифрування, зашифрований текст і ключ. Відкритий текст - це дані до того, як вони були зашифровані. Іншими словами, вихідні дані або повідомлення записуються в комп'ютерній системі у вигляді відкритого тексту. Алгоритм шифрування - це комп'ютерна програма, яка перетворює відкритий текст у зашифровану форму. Зашифрований текст - це дані після застосування алгоритму шифрування. Ключем у процедурі шифрування та розшифрування є унікальні дані, які потрібні як для створення зашифрованого тексту, так і для розшифрування зашифрованого тексту назад до вихідного повідомлення. На рис. 15.1 показано просту схему компонентів системи шифрування та дешифрування (White, 2001).



**Рисунок 15.1 Процедура кодування.**

Найперші системи шифрування використовували один приватний ключ. Іншими словами, один і той самий ключ (або код) використовувався для генерації зашифрованого тексту і для його розшифрування. Проблеми систем з одним приватним (секретним) ключем полягали в тому, що і відправник, і одержувач повинні були мати ключ, а також в тому, що цей ключ повинен був бути захищений від перехоплення або підробки.

**Інфраструктура відкритих ключів** Криптографія з відкритим ключем вирішує основні проблеми систем з одним приватним ключем. У системі з відкритим ключем є два ключі, приватний і публічний. По суті, в цій двоключовій системі дані, зашифровані відкритим ключем, можуть бути розшифровані тільки за допомогою закритого ключа, а дані, зашифровані за допомогою закритого ключа, можуть бути розшифровані тільки за допомогою відкритого ключа. За допомогою криптографії з відкритим ключем зашифровані дані дуже важко зламати (White, 2001). Нижче наведено спрощену ілюстрацію того, як працює криптографія з відкритим ключем.

Медична клініка у великому місті повинна надсилати інформацію про пацієнтів до головної лікарні міста. Спочатку лікарня надсилає відкритий ключ до клініки, а та зберігає відповідний закритий ключ у безпечному місці. Клініка використовує відкритий ключ для шифрування даних перед тим, як відправити їх до лікарні. Тепер тільки лікарня може розшифрувати дані, тому що тільки вона володіє відповідним закритим ключем.

Сьогодні криптографія з відкритим ключем є складовою інфраструктури відкритих ключів (ІВК) - цілої системи, призначеної для практичного використання криптографії з відкритим ключем. ІВК - це поєднання методів шифрування, програмного забезпечення та послуг. Організація охорони здоров'я може впровадити власну модель ІВК або укласти контракт з постачальником послуг додатків (ASP) на розміщення та управління системою ІВК. Одним із потенційних застосувань ІПК в охороні здоров'я є надсилання захищеної електронної пошти. Щоб надіслати захищене електронне повідомлення в середовищі PKI, відправник отримує відкритий ключ одержувача з каталогу в своїй організації. Після отримання відкритого ключа відправник шифрує повідомлення електронної пошти (наприклад, натиснувши кнопку "зашифрувати") і надсилає зашифроване повідомлення. Коли електронний лист потрапляє на комп'ютер одержувача, приватний ключ одержувача автоматично розшифровує повідомлення (Etheridge, 2001).

Існують й інші потенційні можливості використання технології PKI в охороні здоров'я, наприклад, забезпечення безпечного доступу до веб-медичних записів або інших інформаційних систем охорони здоров'я. Одним з прикладів є те, що компанія Marconi Medical Systems, яка виробляє систему архівування і передачі зображень (PACS), інтегрує PKI у свої веб-продукти, щоб забезпечити віддалений доступ через стандартний веб-браузер. PKI також використовується в он-лайн службі виписування рецептів (Etheridge, 2001). Як би чудово не звучала PKI, вона має деякі проблеми. Вона дорога, і багато систем є приватними і не будуть взаємодіяти з іншими системами. Однак, оскільки стандарти HIPAA вимагають вищого рівня безпеки для он-лайн транзакцій у сфері охорони здоров'я, використання технології PKI в охороні здоров'я, ймовірно, зростатиме.

**Pretty Good Privacy** На початку 1990-х років інженер-програміст Філіп Циммерман створив програмне забезпечення для шифрування з відкритим вихідним кодом, яке він назвав Pretty Good Privacy (PGP). PGP має конкретну мету - дозволити звичайній людині створювати та надсилати безпечну електронну пошту та файли даних. PGP використовує криптографію з відкритим ключем і цифрові підписи. Для того, щоб використовувати PGP, робочі станції відправника та отримувача повинні мати однакове програмне забезпечення PGP. Спочатку PGP був доступний через Інтернет. Безкоштовна версія доступна для приватних осіб у Сполучених Штатах від PGP Corporation ([www.pgp.com](http://www.pgp.com/)), а також PGP можна придбати для комерційного використання (White, 2001).

Захист брандмауером

Брандмауер - це "система або комбінація систем, що підтримує політику контролю доступу між двома мережами" (White, 2001). Термін брандмауер може використовуватися для опису програмного забезпечення, яке захищає обчислювальні ресурси, або для опису комбінації програмного забезпечення, обладнання та політик, які захищають ці ресурси (Oz, 2004; Whatis?.com, 2002).

Найчастіше брандмауер встановлюють між внутрішньою мережею організації охорони здоров'я та Інтернетом. Брандмауер не дозволяє користувачам, які отримують доступ до мережі охорони здоров'я через Інтернет, використовувати певні частини цієї мережі, а також не дозволяє внутрішнім користувачам отримувати доступ до різних частин Інтернету (Oz, 2004; Whatis?.com, 2002).

Основними типами брандмауерів є (1) фільтр пакетів, або мережевий рівень, і (2) проксі-сервери, або рівень додатків. Брандмауер з фільтром пакетів - це, по суті, маршрутизатор, запрограмований відфільтровувати одні типи даних і пропускати інші. Ранні версії цих брандмауерів було досить легко обдурити. У міру того, як маршрутизатори ставали все більш досконалими, захист, пропонований цим типом брандмауерів, збільшувався. Проксі-сервер є більш складним брандмауером. Брандмауер проксі-сервера - це програмне забезпечення, яке працює на комп'ютері, що виконує роль воротаря мережі організації. Будь-яка зовнішня транзакція потрапляє в мережу організації через проксі-сервер. Запит на інформацію фактично "зупиняється" на проксі-сервері, де створюється проксі-додаток. Саме цей проксі-сервер входить в мережу організації для отримання запитуваної інформації (White, 2001).

Хоча брандмауери є важливими для загальної безпеки інформаційних систем охорони здоров'я, вони не можуть захистити систему від усіх типів атак. Багато вірусів, наприклад, можуть ховатися в документах, які брандмауер не зможе зупинити.

Перевірка на віруси

Комп'ютерні віруси бувають різних типів. До найпоширеніших типів можна віднести такі (Whatis?.com, 2002)

Файлові інфектори, які приєднуються до програмних файлів так, що при завантаженні програми завантажується і вірус

Системні або завантажувальні інфекції, які заражають системні області дискет або жорстких дисків

Макро-віруси, які заражають програми Microsoft Word, вставляючи в них небажані слова або фрази

Хробак - це особливий тип комп'ютерного вірусу, який зберігає, а потім реплікує себе. Черв'яки зазвичай передаються з комп'ютера на комп'ютер через електронну пошту. Троянський кінь - це деструктивний програмний код, який ховається в іншому програмному коді, що виглядає нешкідливим, наприклад, у макросі або електронному повідомленні (White, 2001).

На щастя, сьогодні на ринку є ефективні антивірусні програми. Ці програми мають три основні функції: сканування на основі сигнатур, термінально-резидентний моніторинг та багаторівневе загальне сканування.

Сканування на основі сигнатур працює шляхом розпізнавання унікального шаблону, або сигнатури, вірусу. Коли з'являються нові віруси, розробники антивірусних програм каталогізують їхні сигнатури. Потім функція сканування сигнатур антивірусного програмного забезпечення сканує програми, повідомлення та файли під час їх завантаження або відкриття, шукаючи збіги з сигнатурами в каталозі. Деякі типи вірусів розроблені таким чином, щоб уникнути виявлення за допомогою функції сканування сигнатур. Антивірусне програмне забезпечення з функцією завершення роботи у фоновому режимі працює у фоновому режимі, тоді як програма працює на передньому плані. Це корисно для пошуку вірусів, які важко виявити, таких як стелс-віруси та поліморфні віруси. Третьою особливістю більшості антивірусних пакетів є багаторівневе загальне сканування. Цей тип перевірки використовує методи "експертного" аналізу для виявлення вірусів, які інші дві функції можуть пропустити (White, 2001).

Перевірка на віруси є важливим компонентом програми захисту медичної інформації. Як ми вже говорили раніше, вірусні атаки є дуже поширеним явищем і можуть спричинити значні збитки та втрату продуктивності. Антивірусне програмне забезпечення є ефективним, якщо каталог вірусів часто оновлюється. Більшість антивірусних програм можна налаштувати на періодичне автоматичне сканування комп'ютерної системи користувача для виявлення та видалення знайдених вірусів.

*Безпека в бездротовому середовищі*

Як ми вже обговорювали в попередніх розділах, бездротові технології змінюють спосіб роботи інформаційних систем охорони здоров'я. Ці технології охоплюють широкий спектр можливостей. Пристрої бездротової локальної мережі (WLAN) дозволяють користувачам легко переносити ноутбуки з місця на місце в межах організації охорони здоров'я. Технології Bluetooth дозволяють синхронізувати дані і надавати спільний доступ до додатків на різних пристроях, таких як клавіатури, принтери та інші периферійні пристрої. Кишенькові пристрої дозволяють віддаленим користувачам синхронізувати дані про персонал і отримувати доступ до мережевих сервісів організацій охорони здоров'я, таких як календарі, електронна пошта і доступ до Інтернету. Ці технології пропонують гнучкість і нові можливості медичним працівникам і людям, які їх підтримують (Karygiannis & Owens, 2002). Однак, впровадження бездротових технологій було відносно швидким, що викликає занепокоєння щодо рівня безпеки, який вони пропонують в такому середовищі, як організація охорони здоров'я. Згідно з офіційним документом, написаним компанією Fluke Networks (2003, стор. l), проблеми з безпекою бездротових мереж "точно такі ж, як і з безпекою дротових мереж. Проблема бездротового зв'язку полягає в тому, що важко обмежити середовище передачі лише тими областями, які ми контролюємо, або лише тими хостами, які ми хочемо бачити в нашій мережі".

Існують специфічні загрози та вразливості, які слід враховувати для бездротових мереж та портативних пристроїв, зокрема такі (Karygiannis & Owens, 2002):

Зловмисники можуть отримати несанкціонований доступ до комп'ютерної мережі організації охорони здоров'я через бездротові з'єднання в обхід захисту брандмауера. Конфіденційна інформація, яка не зашифрована (або зашифрована неякісними методами) і передається між двома бездротовими пристроями, може бути перехоплена і розголошена.

Атаки на відмову в обслуговуванні можуть бути спрямовані на бездротові з'єднання або пристрої. Конфіденційні дані можуть бути пошкоджені під час неправильної синхронізації. Портативні пристрої легко викрасти і вони можуть розкрити конфіденційну інформацію. Внутрішні атаки можливі через спеціальні передачі даних.

Неавторизовані користувачі можуть отримати доступ до бездротової мережі через "піггібекінг" або "воєнне водіння". Користувачі, які просто отримують доступ через незахищене бездротове з'єднання з Інтернетом. Військове водіння передбачає, що несанкціоновані користувачі їздять вулицями міста з антеною та бездротовим комп'ютером у пошуках підключення до Інтернету.

В даний час існує два криптографічних методи для бездротового середовища: WEP (Wired Equivalent Privacy) і новий, більш безпечний WPA (WiFi Protected).

Access). Karygiannis та Owens (2002) відзначають такі проблеми безпеки, пов'язані з WEP: Функції безпеки в продуктах постачальників часто не ввімкнені. Криптографічні ключі короткі. Криптографічні ключі є спільними.

Криптографічні ключі не оновлюються автоматично.

Немає автентифікації користувача - лише автентифікація пристрою.

У відповідь на ці та інші проблеми з безпекою WEP, новий протокол WPA був створений WiFi Alliance, галузевою торговою групою.

Організації охорони здоров'я, які використовують бездротові технології, повинні приділяти пильну увагу аналізу ризиків, пов'язаних з цими технологіями, і зробити заходи безпеки частиною постійного управління ризиками. Як і у випадку з іншими мережами та інформаційними системами, організація повинна знати, де знаходяться загрози та вразливості. Захист портативних пристроїв і портативних комп'ютерів, які зазвичай асоціюються з бездротовою мережею, також створює виклики для організації охорони здоров'я. Необхідно встановити чіткі правила та відповідні санкції для тих, хто порушує ці правила, щоб регулювати завантаження інформації про пацієнтів на такі персональні пристрої. На додаток до стандартних механізмів інвентаризації та призначення відповідальних за портативні комп'ютери, організації охорони здоров'я, можливо, захочуть забезпечити своїх співробітників аксесуарами, які можуть мінімізувати крадіжки: наприклад (Hughes, 2000): кейси, які не містять комп'ютерів.

Кабелі з замками, які чіпляються на столи; якщо цей кабель від'єднати від комп'ютера, то сторонній не зможе його увімкнути. Сигналізації та програмне забезпечення, яке "наказує" комп'ютеру дзвонити і "повідомляти" про своє місцезнаходження.

*Безпека віддаленого доступу*

Організації охорони здоров'я, як і багато інших організацій, що користуються модемом, дозволяють персоналу працювати з дому. Такий віддалений доступ створює додаткові проблеми з безпекою. Насправді сталася низка інцидентів безпеки, пов'язаних з віддаленим використанням ноутбуків та інших портативних пристроїв, які зберігають електронні персональні дані. У відповідь на ці інциденти та потенційний ризик порушень HIPAA через віддалений доступ CMS наприкінці грудня 2006 року випустила настанову з безпеки HIPAA. У наступних таблицях (10.1, 10.2 і 10.3), взятих з цього документу, перераховані потенційні ризики доступу, зберігання і передачі електронних персональних даних при використанні портативних пристроїв у віддалених місцях, а також описані стратегії управління, рекомендовані для зниження цих ризиків.

*Підсумок*

Медична інформація створюється, підтримується та зберігається за допомогою комп'ютерних технологій. Використання цієї технології створює нові проблеми в захисті прав пацієнтів на приватність і конфіденційність, а також вимагає від організацій охорони здоров'я розробки комплексних програм інформаційної безпеки. Публікація остаточних Правил безпеки HIPAA у 2003 році підкреслює важливість захисту медичної інформації та необхідність створення комплексних програм безпеки. Стандарти і специфікації правила HIPAA можуть слугувати основою для організацій охорони здоров'я при розробці ними індивідуальних програм безпеки.

Програми інформаційної безпеки повинні бути розроблені таким чином, щоб протистояти внутрішнім і зовнішнім загрозам інформаційним системам охорони здоров'я, незалежно від того, чи є ці загрози навмисними чи ненавмисними. Програми захисту медичної інформації повинні передбачати адміністративні, фізичні та технічні засоби захисту. У цій главі не тільки викладено вимоги HIPAA до безпеки, але й обговорено багато загальних заходів безпеки, які можуть бути застосовані для мінімізації потенційних ризиків для медичної інформації. i

Посилання:

Вагер, Карен А., Френсіс Вікхем Лі та Джон П. Глейзер. (2009). *Інформаційні системи охорони здоров'я: Практичний підхід до управління охороною здоров'я*.

Друге видання. Сан-Франциско: John Wiley & Sons, Inc.