Доставка на софтуер - особености и процеси

Тема №4

Разпространени стандарти и регулации, гарантиращи определени характеристики на даден продукт и услуга

Част 3: HIPAA / HITECH

Съдържание

1 Въведение

В тази лекция ще се фокусираме върху ключовите аспекти при сигурността на здравните данни, изградени от HIPAA и HITECH. И докато това са закони на САЩ, те са фактически стандарт за този тип данни в световен мащаб. HIPAA (Health Insurance Portability and Accountability Act), създава стандарти за защита на здравната информация, докато HITECH (Health Information Technology for Economic and Clinical Health Act) надгражда HIPAA, фокусирайки се върху ролята на технологиите в здравеопазването. Тези закони не само установяват правила, но и изграждат необходимите технически инструменти, които гарантират сигурността и цялостта на здравната

информация. В днешната ера на дигитализация и обмен на данни, разбирането на тези технически аспекти е от съществено значение за защитата на личната и медицинската информация.

2 Какво е HIPAA?

Health Insurance Portability and Accountability Act, по-известен като HIPAA, е законодателен акт, приет през 1996 г., със съществена роля в опазването на личната и здравната информация в сектора на здравеопазването.

2.1 Цел на HIPAA

Основната цел на HIPAA е да осигури сигурността и поверителността на здравната информация на пациентите. Този закон установява стандарти за обработка и предаване на здравни данни, като налага задължения както върху доставчиците на здравни услуги, така и върху техните бизнес-партньори. HIPAA служи като рамка, в която здравните организации трябва да изграждат и управляват технологии, за да защитят здравната информация на своите пациенти.

2.2 Ключови принципи на HIPAA

- **Право на Пациента:** HIPAA предоставя на пациентите контрол върху тяхната здравна информация, включително правото на достъп и корекция на своите записи.
- **Ограничение на Достъпа:** Законът определя строги правила за ограничаване на достъпа до здравната информация само до лица, които са определени и упълномощени.
- **Сигурност на Информацията:** HIPAA изисква изпълнението на технически и организационни мерки за сигурност, включително шифроване, контрол на достъпа и одит на системите.

2.3 Значение за Здравните Организации

За здравните организации, спазването на HIPAA е задължително. Те трябва да изградят и поддържат сигурни системи и процедури, които гарантират конфиденциалността и цялостта на здравната информация. Обхванатите субекти подпадат под шапката на HIPAA включват лекари, болници, зъболекари, здравни фондове и други.

2.4 Възможни последици от нарушения

Нарушенията на HIPAA не са без последствия. Законът предвижда сериозни глоби при несъответствие, но и по-важното - те могат да доведат до загуба на доверие от страна на пациентите. Изграждането на стриктни мерки за сигурност и спазването на стандартите на HIPAA не само предпазват здравните организации от финансови загуби, но и укрепват доверието във връзката с пациентите и партньорите.

3 Какво е HITECH?

Законът HITECH (Health Information Technology for Economic and Clinical Health Act) от 2009 г. засилва прилагането на HIPAA по няколко начина. Най-важното е, че HITECH разширява обхвата на Правилото за сигурност на HIPAA до бизнес-партньорите на обхванатите субекти, които също трябваше да се съобразяват с определени стандарти на Правилото за поверителност и новото Правило за уведомяване при нарушение. Също така въвежда по-строги наказания за неспазване на HIPAA. Въпросните бизнес-партньори включват доставчиците на услуги, които съхраняват или обработват медицински данни. HITECH адаптира HIPAA към съвременните технологични предизвикателства като увеличаващите се заплахи от кибератаки и несъответствие със стандартите за сигурност.

3.1 Цели на HITECH

Петте цели на Закона HITECH са описани като петте цели на здравеопазването в САЩ:

1. Подобряване на качеството, безопасността и ефективността
2. Ангажиране на пациентите в техния процес на грижа
3. Увеличаване на координацията на грижата
4. Подобряване на здравното състояние на населението
5. Гарантиране на поверителност и сигурност

За постигане на тези цели, HITECH стимулира приемането и използването на технологии за здравна информация, дава възможност на пациентите да проявяват активен интерес към своята здравна информация, изгражда основите за разширяване на обмена на здравна информация и засилва разпоредбите за поверителност и сигурност на HIPAA.

3.2 Значение за Здравните Организации

HITECH стимулира здравните организации да приемат електронни здравни записи (Electronic health record / EHR) и подобряват защитата на поверителността и сигурността на здравните данни. Това се постига чрез финансови стимули за приемане на електронни здравни записи и увеличаване на наказанията за нарушения на Правилата за поверителност и сигурност на HIPAA.

HITECH също така помага за гарантиране, че здравните организации и техните бизнес-партньори се съобразяват с Правилата за поверителност и сигурност на HIPAA, въвеждат защитни мерки за поддържане на поверителността и сигурността на здравната информация, ограничават използването и разкриването на здравната информация и изпълняват задължението си да предоставят на пациентите копия от техните медицински записи по заявка.

Законът не прави съответствието с HIPAA задължително, тъй като това вече е изискване, но въвежда ново изискване за Обхванатите субекти и Бизнес-партньори да докладват за нарушения на данните – което в крайна сметка позволява на регулатора да засили прилагането срещу организации, несъответстващи със законодателството.

3.3 Възможни последици от нарушения

HITECH въвежда по-строги наказания за неспазване на HIPAA като допълнителна стимулация за здравните организации и техните бизнес-партньори да спазват Правилата за поверителност и сигурност на HIPAA и да финансират засилени действия за прилагане от отделението за граждански права на Министерството на здравеопазването и социалните услуги.

4 Структура на HITECH

HITECH съдържа четири секции (A-D).

Секция A се отнася до насърчаването на технологиите за здравна информация и се разделя на две части. Част 1 се отнася до подобряване на качеството, безопасността и ефективността на здравната грижа. Част 2 се отнася до прилагането и използването на стандартите за технологии за здравна информация и докладите.

Секция B обхваща тестването на технологиите за здравна информация, секция C обхваща финансирането с грантове и заеми, а секция D обхваща поверителността и сигурността на електронната здравна информация. Секция D също се разделя на две части. Част 1 се отнася до подобряването на поверителността и сигурността на технологиите за защитената здравна информация (Protected health information / PHI), а Част 2 обхваща връзката между Закона HITECH и другите закони.

5 Как HITECH води до HIPAA съответствие на бизнес-партньорите

Според първоначалните Правила за поверителност и сигурност на HIPAA, Бизнес-партньорите на Обхванатите субекти по HIPAA имат "договорна задължености" да се съобразяват с HIPAA. Преди приемането на Закона HITECH през 2009 г., този задължителен стандарт не е активно прилаган, а

Обхванатите субекти могат да избегнат санкции в случай на нарушение на защитата на здравната информация от страна на Бизнес-партньор, като твърдят, че не са знаели, че Бизнес-партньорът не се съобразява с HIPAA. Поради факта, че Бизнес-партньорите не могат да бъдат пряко глобявани за нарушения по HIPAA, мнозина не спазват изискванията на HIPAA и поставят на риск милиони здравни записи.

Законът HITECH от 2009 г. прилага Правилата за сигурност и поверителност на HIPAA и към Бизнес-партньорите, като ги прави директно отговорни за собственото си съответствие с HIPAA. Бизнес-партньорите трябва вече да подписват Споразумение на Бизнес-партньор с Обхванатия субект, от името на който обработва здравна информация, и са предмет на същите правни изисквания като Обхванатия субект за защита на здравната информация и предотвратяване на нарушения на данните. Бизнес-партньорите също трябваше да докладват за нарушения на данните на Обхванатите субекти.

Последното Комплексно Правило на HIPAA от 2013 г. (HIPAA Final Omnibus Rule of 2013) задълбочава изискванията за съобразяване на Бизнес-партньорите. След приемането на Комплексното Правило, Бизнес-партньорите стават предмет на проверки по HIPAA, и граждански и наказателни глоби могат да бъдат налагани директно на Бизнес-партньорите за несъответствие с правилата на HIPAA, независимо дали е станало нарушение на данните или не.

6 Постигане на съответствие

В общия случай съответствието с HIPAA означава покриване на стандартите, изискванията и спецификациите за прилагане на Регламентите за административно опростяване на HIPAA.

Освен това Обхванатите субекти и Бизнес-партньорите са задължени да се защитават срещу всички разумно предвидени използвания и разкривания на PHI (защитена здравна информация), които не са разрешени от Правилото за поверителност, и срещу всички разумно предвидени заплахи за сигурността на PHI, които не са обхванати от Правилото за сигурност - дори ако не съществува конкретен стандарт, свързан с непозволеното използване или разкриване или заплахата за сигурността.

6.1 Оценка на риска при HIPAA

Липсват насоки относно това кои рискове следва да бъдат оценени и как следва да се анализират оценките на риска.

Министерството на здравеопазването и социалните услуги (HHS) пояснява, че липсата на предоставена "специфична методология за анализ на риска" се дължи на факта, че Обхванатите субекти и Бизнес-партньорите са с различни размери, възможности и сложности.

Въпреки това HHS предоставя насоки за целите на оценката на риска за HIPAA:

1. Идентифициране на PHI, която организацията създава, получава, съхранява и предава - включително PHI, споделена с консултанти, доставчици и бизнес-партньори.

2. Идентификация на човешките, природните и екологичните заплахи за цялостта на PHI - човешките заплахи включват както умишлените, така и неумишлени.

3. Оценка на мерките, предприети за защита срещу заплахи за цялостта на PHI и вероятността от "разумно предвидено" нарушение.

4. Определяне на потенциалните последици от нарушение на PHI и определяне на ниво на риск за всяко потенциално събитие въз основа на средното ниво на допустимата вероятност и въздействие.

5. Документиране на резултатите и въвеждане на мерки, процедури и политики, ако е необходимо, за постигане и поддържане на съответствие с HIPAA.

6. Оценката на риска за HIPAA, обосновката за последващо въведените мерки, процедури и политики, както и всички документи за политики, трябва да бъдат съхранявани за минимум шест години.

Оценката на риска за HIPAA не е еднократно изискване, а редовна задача, необходима за гарантиране на продължителното съответствие с HIPAA.

Оценката на риска за HIPAA и анализът на нейните резултати ще помогнат на организациите да анализират много от другите аспекти на постигане на съответствието и следва да бъдат ревизирани всякога, когато настъпят промени в работната сила, работните практики или технологиите.

В зависимост от размера, възможностите и сложността на организацията, изготвянето на изцяло комплексна оценка на риска за HIPAA може да бъде изключително дълъг процес.

6.2 Правило за поверителност / HIPAA Privacy Rule

HIPAA Privacy Rule установява национални стандарти за защита на медицинските записи на лица и друга индивидуално идентифицируема здравна информация (дефинирана като PHI, когато се поддържа или предава от Обхванат субект) във всякакъв формат, в който тя се създава, получава, поддържа или предава (например, устно, писмено или електронно).

Правилото изисква подходящи гаранции за защита на поверителността на PHI и определя ограничения за използването и разкриването на такава информация без разрешението на индивида.

Правилото за поверителност също така предоставя на лицата права върху техните PHI, включително правото да получат копие на поддържаната в отделен запис PHI, да поискат корекции при наличие на грешки и да прехвърлят част или целия поддържан PHI в отделен запис на друг доставчик.

Лицата също така имат право да поискат доклад за разкриванията - информация за използванията или разкриванията на PHI през последните шест години, освен определени позволени или упълномощени разкривания.

Въпреки че Privacy Rule се отнася до по-малко организации отколкото Security Rule, най-добре е да започнете по пътя на съответствието с HIPAA с правилата, свързани с поверителността и правата на индивидите. Това се дължи на факта, че Privacy Rule е основата за всяко друго правило на HIPAA; и дори ако вашата организация не е задължена да спазва разпоредбите на Privacy Rule, разбирането на това, което те са и тяхната цел, е практически необходимо за съответствие с другите правила на HIPAA.

Следователно, следният списък за съответствие с HIPAA Privacy Rule следва да бъде разглеждан като отправна точка за всеки следващ списък за съответствие с HIPAA, който може да бъде по-подходящ за дадена организация.

1. Назначаване на отговорно лице за поверителността на HIPAA, отговорно за разработването, въвеждането и прилагането на политики съгласно HIPAA.

2. Разбиране какво е PHI, как може да бъде използвана и разкривана в съответствие с HIPAA и кога е необходимо упълномощаване от страна на индивида.

3. Идентифициране на рисковете за поверителността на PHI и въвеждане на гаранции за минимизиране на рисковете до "разумно и подходящо" ниво.

4. Разработване на политики и процедури за използване и разкриване на PHI в съответствие с HIPAA и за предотвратяване на нарушенията на HIPAA.

5. Разработване на политики и процедури за получаване на разрешения и предоставяне на възможност на лицата да се съгласят или да възразят, когато е необходимо.

6. Разработване и разпространение на Обявление за поверителност, обясняващо как организацията използва и разкрива PHI и представящо правата на лицата.

7. Разработване на политики и процедури за управление на исканията за достъп на пациенти (до техния PHI), исканията за корекции и исканията за трансфер на данни.

8. Разработване на процедури за служители за докладване на нарушения на HIPAA и за организацията за изпълнение на изискванията за съобщаване за нарушения.

9. Обучение на служителите по политиките и процедурите, отнасящи се до техните роли, и по общото съответствие с HIPAA.

10. Разработване и разпространение на политика за санкции, представяща санкции за несъответствие с организационните политики на HIPAA.

11. Извършване на необходимата проверка на Бизнес-партньорите, преглеждайки съществуващите споразумения с Бизнес-партньорите и коригирайки ги при необходимост.

12. Разработване и документиране на план за реакция при спешна ситуация, която повреждa системи или физически места, в които се поддържа PHI.

6.3 Правило за сигурност / HIPAA Security Rule

HIPAA Security Rule засяга стандарти, предназначени да гарантират поверителността, цялостта и наличността на ePHI (електронно създадена, получена, поддържана или предавана защитена здравна информация).

6.3.1 Общи правила

Този първи раздел на HIPAA Security Rule често се пренебрегва, въпреки че съдържа няколко ключови указания за Обхванати субекти и Бизнес-партньори относно техните задължения за съответствие. Например, Общите правила предписват, че Обхванатите субекти и Бизнес-партньорите трябва:

- да се защитават от всяка разумно предвидима заплаха или опасност за сигурността или целостта на ePHI.
- да се защитават от всяка разумно предвидима употреба или разкриване на PHI, които не са разрешени от Privacy Rule.
- да се подсигури съответствие с Security Rule от страна на служителите.

Това означава, че организациите трябва да идентифицират разумно предвидими заплахи и опасности, потенциални неразрешени употреби и разкривания, да въведат мерки за защита срещу тях и след това да наблюдават дейностите, за да се уверят, че служителите спазват политиките и процедурите по Security Rule, въведени от организацията.

Мерките на Security Rule (разглеждаме ги в следващите секции) предоставят минималните мерки, които трябва да се въведат, за да се спазят тези указания, но е важно да се знае, че ако съществува разумно предвидима заплаха или опасност, която не е обхванатa от тези минимални мерки, организациите са отговорни за разработването и въвеждането на допълнителни мерки.

По този начин Общите правила позволяват "гъвкав подход". Клаузата за гъвкавост на подхода дава на организациите свобода да определят кои мерки за сигурност са подходящи за намаляване на заплахи, опасности и риска от неразрешени употреби и разкривания в зависимост от техния размер, наличните възможности и критичността на идентифицираните рискове.

Въпреки това гъвкавостта на подхода не извинява Обхванатите субекти и Бизнес-партньори от спазване на всички мерки на Security Rule, освен ако реализацията е "адресируема" и са изпълнени условията, че мярката не е разумна или подходяща или еквивалентна алтернативна мярка би била поне толкова ефективна.

6.3.2 Административни мерки за осигуряване на сигурността

Административните мерки са основата на съответствието с Security Rule, тъй като изискват определянето на Офицер по сигурността с отговорност за провеждане на анализи на риска, въвеждане на мерки за намаляване на рисковете и уязвимостите, обучение на служителите, надзор на непрекъснатостта на ИТ, и сключване на споразумения с бизнес-партньори.

Има някои области, където ролите на Офицер по сигурността и Офицер по поверителността се пресичат, тъй като и двете са задължени да разработват план за спешна ситуация, за да гарантират непрекъснатостта на бизнеса, и да извършват проверка за бизнес-партньорите.

Това вероятно е така, защото някои бизнес-партньори може да не подлежат на Privacy Rule, но трябва да гарантират непрекъснатостта на бизнеса и да сключват споразумения за бизнес-партньор.

Стандарти и Допълнителна Информация

- **Процес за Управление на Сигурността** - Организациите трябва да провеждат анализи на риска, въвеждат мерки за намаляване на рисковете и уязвимостите, въвеждат политика за санкции за служителите и въвеждат процедури за преглед на системната дейност.
- **Отговорности за Сигурност** - Определяне на Офицер по сигурността по HIPAA, отговорен за разработването, въвеждането и спазването на процедури и политики по Security Rule. Този човек може да бъде същият като Офицер по поверителността по HIPAA.

- **Сигурност на служителите** - Служителите трябва да получат одобрение, преди да имат достъп до системи, съдържащи ePHI, и трябва да се въведат мерки за ограничаване на достъпа до ePHI и прекратяване на достъпа, когато променят ролите си или приключват работната си дейност.
- **Управление на Достъпа до Информация** - Този стандарт се отнася до хибридни и асоциирани организации, за да се гарантира, че ePHI се достъпва само от служители на "покритите" организации и не от служители на родителска, съвместна или асоциирана организация.
- **Осъзнатост и Обучение по Сигурност** - Служителите - дори тези, които нямат достъп до ePHI, трябва да участват в програма за обучение по сигурност. Този стандарт включва също напомняния за сигурност и управление на пароли.
- **Процедури при Инциденти със Сигурността** - Стандартът изисква от Обхванати субекти и Бизнес-партньори да въведат мерки за съобщаване, реагиране и документиране на резултатите от инциденти със сигурността (Забележка: Не се ограничава до инциденти, свързани с киберсигурност).
- **План за Спешна Ситуация** - Създаване (и тестване) на политики и процедури за реагиране на спешна ситуация. Политиките и процедурите трябва да включват план за резервно копие на данни, план за възстановяване след бедствие и план за работа в режим на спешна ситуация.
- **Периодични Оценки** - Този стандарт изисква от Обхванатите субекти и Бизнес-партньори периодично преглеждане на политиките, процедурите и въведените мерки, за да се съобразят с Security Rule - включително споразуменията с бизнес-партньори.

6.3.3 Физически мерки за осигуряване на сигурността

Физическите мерки се съсредоточават върху физическия достъп до ePHI, независимо от местоположението ѝ.

ePHI може да се съхранява в отдалечен център за данни, в облака или на сървъри, които се намират в сградите на организацията.

Физическите мерки също така определят как работните станции и мобилните устройства трябва да бъдат защитени от неоторизиран достъп.

Стандарти и Допълнителна Информация

- **Контрол на Достъпа до Обектите** - Въпреки че този стандарт се отнася до физическия достъп до електронни информационни системи и сградите, в които се намират, трябва да се предприемат мерки, за да се ограничи физическият достъп до хартиени PHI, когато това е възможно.
- **Използване на Работните Станции** - Има различни тълкувания на този стандарт, като най-сигурното тълкуване е забраната на не-делова дейност на работните станции и устройства, използвани за създаване, получаване, поддържане или предаване на ePHI.
- **Сигурност на Работните Станции** - Този стандарт изисква от Обхванатите субекти и Бизнес-партньори да внедрят средства за защита, така че физическият достъп до работните станции и устройствата да бъде ограничен само до членове на работната сила с подходящо разрешение.
- **Контроли за Устройствата и Носителите на Информация** - Спецификациите за изпълнение, свързани с този стандарт, включват изхвърляне или повторна употреба на носителите, на които е съхранена ePHI, и поддържане на инвентар на устройствата и носителите, използвани от организацията за достъп до ePHI.

6.3.4 Технически мерки за осигуряване на сигурността

Техническите мерки за сигурност са предназначени да гарантират, че всеки, който има достъп до ePHI, е този, за когото се представя, и че прави това, за което е предназначен. Ако възникне проблем поради случайно или злонамерено действие, проблемът трябва да бъде идентифициран и отстранен възможно най-бързо.

Стандарти и Допълнителна Информация

- **Контрол на Достъпа** - Този стандарт не само се отнася до идентификацията на потребителя и управлението на паролите, но включва и спецификации за автоматично излизане, криптиране и процедури за спешен достъп.
- **Контроли за Отчетност** - Стандартът за контрол на отчетността изисква от Обхванатите субекти и Бизнес-партньори да внедрят софтуер, който записва събития и проучва активността на системите, съдържащи ePHI.
- **Контроли за Цялост** - Като допълнение към горния стандарт, трябва да се внедрят контроли, за да се гарантира, че ePHI не бъде променяно или унищожено неправомерно. Това е толкова важно за смекчаване на заплахите от злонамерени вътрешни лица, колкото и за външни заплахи.
- **Автентикация на Субекта** - Този стандарт е практически идентичен с изискванията за идентификация на потребителя в стандарта за контрол на достъпа и демонстрира важността на внедряването и прилагането на ефективна политика за управление на пароли.
- **Сигурност при Предаването** - За разлика от стандарта за контрол на цялостта, който се отнася до ePHI, когато бъде достъпено от оторизиран потребител, този стандарт изисква въвеждане на мерки, за да се гарантира цялостта и сигурността на ePHI по време на трансфер и предотвратяване на неоторизираното унищожаване или прихващане.

6.3.5 Организационни Изисквания

Организационните Изисквания на Правилото за Сигурност са от значение за повечето Обхванати субекти и Бизнес-партньори, тъй като обхващат Споразумения с Бизнес-партньори.

Споразуменията с Бизнес-партньори са разгледани и в други разпоредби за Административно Опростяване, но за организации, участващи в бизнес отношения, при които се разкрива ePHI, е важно да бъдат осведомени за този конкретен раздел, защото той предписва:

- Споразуменията с Бизнес-партньори трябва да предвиждат, че Бизнес-партньорът се съобразява с приложимите части от Правилото за Сигурност,
- Бизнес-партньорите, които възлагат на подизпълнители услуги, при които се разкрива ePHI, трябва да сключат споразумение с подизпълнителя, и
- Бизнес-партньорите ще докладват всеки инцидент за сигурност - включително, но не само, нарушения на незащитена ePHI - на Обхванатия субект, с когото е сключено Споразумението.

Съществуват допълнителни изисквания в Организационните Изисквания, когато здравен фонд разкрива ePHI на спонсор на плана, и те са много подобни на Организационните Изисквания, свързани с хибридни субекти.

6.3.6 Изисквания за Сигурност на HIPAA

Въпреки че нито един стандарт в Правилото за Сигурност не е по-важен от друг, някои са ключови, защото - без тях - би било трудно да се спази Правилото в пълнотата му. Следователно сега ще разгледаме основни изисквания за сигурност на HIPAA.

1. Да се определи HIPAA Офицер по сигурността. Ролята може да бъде възложена на Офицер по поверителността; но в по-големите организации е най-добре да се определи ролята на член на екипа по информационните технологии.
2. Да се определят системите, създаващи, получаващи, поддържащи или предаващи ePHI, и да се защитят от неоторизиран достъп от други части на IT инфраструктурата на организацията.
3. Да се внедрят мерки, които ограничават заплахите от злонамерени софтуери, рансъмуер и фишинг. Например, модерни филтри за електронна поща и Интернет със способности за откриване на злонамерени URL адреси.

4. Да се установят кои служители трябва да имат достъп до ePHI и да се внедрят контроли за достъп на база роли, за да се предотврати достъпът на потребители до повече ePHI, отколкото трябва.

5. Да се внедрят системи за верификация на идентичността на служителите, за да се спазят изискванията за физически достъп, сигурност на работните станции и записи на събитията на Правилото за Сигурност.

6. Да се направи инвентар на устройствата, използвани за достъп до ePHI и на носителите, на които се съхранява. Да се осигури наличие на система за регистриране на всяко придвижване на устройства и носители.

7. Да се увери, че всички устройства, използвани за достъп до ePHI - включително отдалечени и лични устройства - са заключени с PIN и са активирали автоматичният logout, за да се предотврати неоторизиран достъп.

8. Да се въведат процедури за упълномощени служители да докладват инциденти за сигурност или да повдигат въпроси за сигурност до Офицера по сигурността или Оперативния Център за Сигурност.

9. Да се внедрят програми за обучение и осведоменост за сигурност за всички служители, които включват как да повдигат въпроси за сигурност и процедури за докладване на инциденти.

10. Да се разработи политика за санкции, обясняваща санкциите за нарушаване на политиките за сигурност на организацията, и да се разпространи сред всички служители (дори тези без достъп до ePHI).

11. Да се разработи план за противодействие на предвидими събития, които могат да застрашат поверителността, цялостта и наличността на ePHI, и да се тества планът за всеки вид събитие.

12. Да се прегледат съществуващите Споразумения с Бизнес-партньори, свързани с разкриването на ePHI, и да се заменят тези, които не съответстват на Организационните Изисквания на Правилото за Сигурност на HIPAA.

6.4 Правилото за Известяване при Нарушение на HIPAA

Всички организации, които създават, получават, поддържат или предават PHI или ePHI, трябва да се съобразяват с Правилото за Известяване при Нарушение на HIPAA. Това включва организации, които не подлежат на Правилата за Поверителност и Сигурност, като доставчици на лични здравни записи ("PHRs"), свързани със здравните записи обекти (например fitness tracking услуги, изпращащи данни към PHR или имащи достъп до данни във PHR) и доставчици на услуги от трета страна.

Следователно всички организации трябва да бъдат готови да уведомяват лицата, съответната федерална агенция и - в някои случаи - местните медии, когато настъпи нарушение с незащитена PHI/ePHI. В такива случаи е важно да се изпълнят всички приложими изисквания на Правилото за Известяване при Нарушение, дори ако нарушението засяга здравния запис на единично лице.

Въпреки това, преди да се предприемат процедурите за известяване при нарушение, е важно организациите да установят дали нарушението е подлежащо на известяване или не. Ненужното докладване на нарушение на данните вероятно ще доведе до ненужно разследване, което, дори ако не се установи нарушение, ще доведе до някаква степен на нарушение на бизнеса, освен ненужни тревоги за засегнатото лице (лица).

Поради това организациите трябва да се уверят, че всяко нарушение е подлежащо на известяване, като първо проведат оценка на риска или използват инструмент за вземане на решения за нарушение на HIPAA/Формуляр за оценка на риска при нарушение на HIPAA, за да се определи:

- Дали ePHI е шифрована и следователно нечетима, неразбираема и неизползваема?
- Ако не, какви здравни информации и идентификатори са изложени в нарушението?
- Кой (ако е известен) незаконно е придобил, получил достъп или разгледал PHI/ePHI?
- Каква е вероятността данните да бъдат допълнително използвани или разкривани?
- Какви мерки са предприети, за да се ограничат последиците от нарушението?

Ако нарушението е подлежащо на известяване, лицата трябва да бъдат уведомени за нарушението в рамките на шестдесет дни. Уведомлението за нарушението трябва да включва информация за това, какви данни са разкрити, какви мерки предприема организацията, за да се ограничат ефектите от нарушението и предотвратят допълнителни инциденти за сигурност, както и как лицата могат най-добре да се предпазят от кражба или измама.

Ако нарушението засяга по-малко от 500 лица, организациите имат до края на всяка календарна година да уведомят Комисията по граждански права (Office for Civil Rights / OCR) на HHS или Федералната търговска комисия. Нарушения, засягащи 500 или повече лица, трябва да бъдат съобщени на съответната агенция и местните медии в рамките на шестдесет дни - неспазването на това може да предизвика по-строги глоби за нарушение на HIPAA от Комисията по граждански права на HHS или глоба от Федералната търговска комисия.

6.5 HIPAA одит

Въпреки че програмата за аудит на OCR може да не е толкова активна, колкото преди няколко години, все още е полезно организациите да се подготвят за одит на съответствието, тъй като документацията, изисквана при одит, е същата като тази, изисквана при разследване, проведено от федерална агенция в отговор на нарушение на данните или жалба. Няма да се фокусираме на този аспект.

7 Фокус върху информационните технологии

Съгласно "гъвкавостта на подхода" на Security Rule, факта, че някои по-малки организации имат ограничени ресурси, и че някои по-големи организации се сблъскват с уникални предизвикателства в съответствието, няма универсална процедура за съответствие на информационните технологии с HIPAA. Въпреки това може да разгледаме някои най-добри практики, които могат да помогнат на ИТ отделите да отговорят на изискванията на HIPAA.

1. Прилагане на политика за пароли, изискваща използването на уникални и сложни пароли за всеки акаунт и въвеждане на политиката със задължително многократно удостоверяване (2FA / MFA), където е практично.

2. Автоматизация на надзора и докладването, колкото е възможно, за да се намали административната тежест от съответствието на потребителите и управлението на заплахи.

3. Тестване на плановете за реагиране при инциденти и възстановяване след бедствие за всеки възможен случай. Подсигуряване, че всички членове на екипа разбират своите роли по време на такива събития.

4. Разделяне на инфраструктурата на данните и системния слой, за да се поддържа цялостта на системата и да се изолират атаките върху системата.

5. Внедряване на технологии за кодиране или блокчейн, за да се предотврати намесата и да се подпомогнат усилията за съответствие с цел гарантиране на цялостта на ePHI.

6. Подготовка за възможността за компрометиране на потребителски пароли и готовност за изключване на компрометираните акаунти отдалече.

7. Документиране на потоците на данни – включително тези към/от бизнес-партньорите – за опростяване на оценките на риска и анализите и по-ефективно идентифициране на заплахите за ePHI.

8. Не бива да се предполага, че всички потребители имат едно и също ниво на знание, осведоменост или податливост. Трябва да се идентифицират къде съществуват слабости в потребителите, за да се изградят по-силни защити срещу кибератаки.

8 HIPAA Сертификация

Сертификацията по HIPAA е процес, при който независима трета организация извършва одит на медицинска организация или практика, за да удостовери, че са изпълнени физическите, техническите и административни гаранции, изисквани за съответствие с HIPAA. След успешен одит се издава официален документ, който сигнализира за завършването на процеса по съответствие с HIPAA. Въпреки че Министерството на здравеопазването и службата по граждански права, отговорна за прилагането на HIPAA, не признават или подкрепят конкретни курсове или сертификати по HIPAA като изпълняващи задълженията по законите на HIPAA, сертификацията по HIPAA доказва, че организацията е участвала и завършила процеса по съответствие с HIPAA и има стойност в практиката.

8.1 Изисквания за Сертификация по HIPAA за Обхванати Субекти

За да бъде сертифицирана като съответстваща на HIPAA, трети организации за съответствие ще преглеждат седем области на съответствие:

- Съответствие с административните, техническите и физическите гаранции на Правилника за Сигурност на HIPAA. Това включва (но не се ограничава до) одит на активи и устройства, анкета за анализ на риска за ИТ, одит на физическото място, одит на стандартите за сигурност, одит на стандартите за поверителност и одит на поверителността по HITECH секция D.
- Планове за отстраняване на недостатъците, идентифицирани в гореспоменатите одити.
- Политики и процедури за съответствие с регулаторните изисквания на HIPAA и документиране на "искрено усилие" за съответствие.
- Програма за обучение на служителите, която включва разбирането на служителите за гореспоменатите политики и процедури.
- Одит за документация, за да се гарантира, че документацията, изисквана от HIPAA, се поддържа и е достъпна.
- Управление на споразуменията с делови партньори и процедури за проверката им.
- Процедури за управление на инциденти в случай на нарушение на данни или подлежащо на докладване нарушение на HIPAA.

Поради процесите, свързани с одита на съответствие с Правилника за Сигурност на HIPAA, изискванията за сертификация по HIPAA не могат да бъдат изпълнени веднага. Също така е невъзможно да се постави времева рамка за постигане на сертификация по HIPAA без да се знае какви недостатъци могат да бъдат идентифицирани по време на процесите на одит и характера на плановете за отстраняване, необходими за тяхното решаване.

8.2 Изисквания за Сертификация по HIPAA за Бизнес-партньори

Изискванията за сертификация по HIPAA за бизнес-партньори са много сходни с гореспоменатите, но се насочват към характера на предоставените услуги за Обхванатите Субекти. Важно е да се отбележи, че въвеждането на програма за обучение по сигурност и осведоменост е за всички служители - не само за тези, занимаващи се с предоставянето на услуга на Обхванатите Събития.

Обикновено потенциалните бизнес-партньори на Обхванатите Субекти по HIPAA преминават през одити от страна на трети страни, които се занимават със съответствие с HIPAA, за да потвърдят, че техните продукти, услуги, политики и процедури отговарят на стандартите на HIPAA. Одитите са полезни за увереността на Обхванатите Субекти, тъй като потвърждават съответствието с HIPAA към момента на провеждане на одита.

Въпреки това, за бизнес-партньори, непознаващи сложността на HIPAA, е вероятно, че ще им е необходима помощ, за да станат съответстващи. Поради тази причина може да бъде важно да се избере трета страна, специализирана в съответствие с HIPAA, която не само предоставя услуги по сертификация по HIPAA, но също така помага на бизнес-партньорите да внедрят ефективни програми за съответствие с HIPAA.

9 Заключение

HIPAA и HITECH са популярни и важни закони, превърнали се в стандарти за работа с един от най-чувствителните видове информация. Въпреки, че е американски закон, много компании прибягват до съответствие с него, главно поради желанието да продават софтуера си на компании в здравния сектор на САЩ - сектор, в който има голям потенциал и сериозно количество финансови средства.