

Очень краткий взгляд разработчика HIPAA-приложений... Только самое основное... Не претендую на абсолютную истину, возможно что-то упускаю. Буду благодарен другим разработчикам HIPAA-compliant софта за дополнения и поправки.

1. HIPAA защищает любую персональную информацию людей (пациентов, клиентов). Всё что может идентифицировать пациента должно быть закрыто внутри ПО. Должна пресекаться любая утечка персональных пользовательских данных. Должны изначально устанавливаться правила предотвращающие возможность мошенничества и кражи данных.

Если ПО предусматривает разные уровни привилегий для отдельных пользователей, пользователи не должны видеть ничего свыше своего уровня привилегий. Неавторизованные пользователи не должны видеть ничего.

2. При этом, несмотря на тотальную секьюрность данных внутри приложений, должна предоставляться возможность скачивать информацию о пациентах на физические носители, типа флешек. Для передачи данных аудиторам.

Все документы о здоровье пациентов должны быть подготовлены к распечатке (желательно в PDF) и содержать информацию о специалисте (докторе), который подготовил эту информацию, в т.ч. его подпись. В идеале написанную от руки. Некоторые страховые компании конкретно требуют *hand-written signature*, некоторые довольствуются тем, что указано имя авторизованного специалиста каким-то шрифтом напоминающим подпись, но подпись специалиста на документах касающихся записей о чьём-либо здоровье должна быть всегда.

Прямой доступ к данным по сети аудиторам давать не обязательно. Желательно, с учётом всех мер предосторожности, цифровых подписей, многоуровневой авторизации и т.д., но не обязательно, потому что всё равно есть опасность утечки данных. Достаточно скачивать данные по запросу аудиторов-страховиков на физический носитель и передавать им под расписку.

Собственно, весь HIPA-акт создан для страховых компаний. Для возможности простой и унифицированной проверки медицинских данных, для аудита траты страховых денег.

3. Сложности при разработке... Запрещается интеграция с любыми 3rd-party API. Это вообще никак. HIPAA-compliant приложения нельзя ни интегрировать с Гугл-календарём, ни вставлять фейсбук-пиксели, ни сделать авторизацию для пользователей при помощи соцсетей. Даже простую капчу при помощи сторонних сервисов делать нельзя. Приложение с гугл-капчей уже не HIPAA-compliant. Потому что возможен доступ стороннего приложения ко страницам/формам с медицинскими данными... Да что там капча, простое видео с ютюбика в HIPAA-compliant веб-приложение вставить нельзя. Всё только своё внутреннее ставится. Шрифты с внешних ресурсов и посторонних CDN использовать тоже нельзя. Гугл-аналитику использовать нельзя.

Нельзя использовать адресацию, которая содержит персональные данные. Адреса типа «domain/path/client-name» запрещены, т.к. имя клиента остаётся в истории браузера. Веб адреса с параметрами типа «адрес-страницы?param=страховой номер&какие-то=медицинские-данные» тоже запрещены.

4. Не уверен, как проходит аттестация HIPAA-приложений, если она есть. Это проходит мимо меня. Но мои HIPAA-compliant веб-приложения сходу отвергаются заказчиком, если в ответе веб-сервера на любые запросы не стоит такой Content-Security-Policy:

```
Content-Security-Policy: default-src 'self'; connect-src 'self'; style-src 'self'; script-src 'self' 'nonce-TEMPORARY-NONCE'.
```

И всё. Все посторонние ресурсы будут резаться браузером. Инлайн-скрипты и инлайн-css невозможны. Внешние скрипты доступны только с того же домена. <script>-блоки на страницах допустимы только если в них стоит сгенерированный временный нонс. Такие приложения проходят.

UPD. Чуть не забыл... По каждому действию ведутся логи. Кто когда входил, с какого устройства, из какого места (желательно), в какое время, какое действие совершил. Буквально каждое действие пользователя оставляет след в логах. Каждый запрос на получение и тем более на изменение информации.