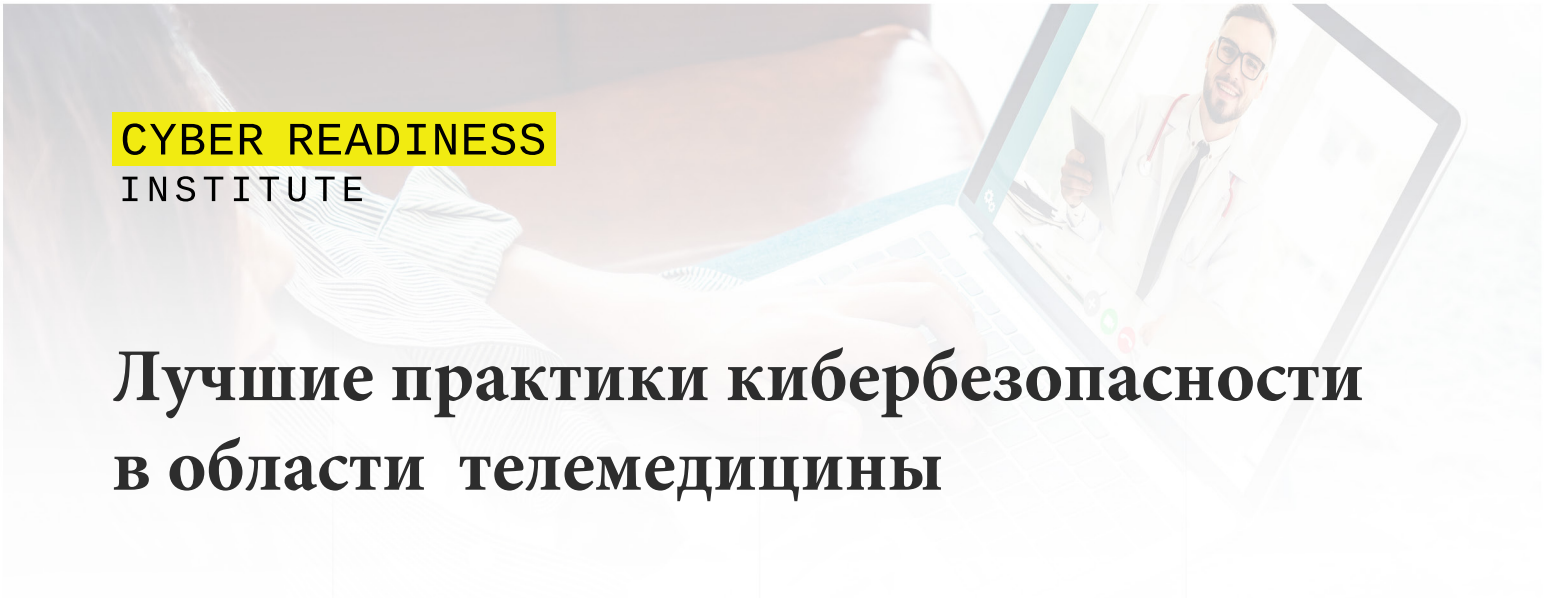
CYBER READINESS
INSTITUTE



Лучшие практики кибербезопасности в области телемедицины

Ландшафт здравоохранения сейчас выглядит иначе, чем восемь месяцев назад. Телемедицина стала более распространенной, чем когда-либо прежде, и существуют новые правила, которые необходимо понять и внедрить в своей практике. Несмотря на все эти изменения, одна проблема остается неизменной: наша система здравоохранения содержит огромное количество персональных, чувствительных и конфиденциальных данных.

Вопросы доступа и безопасности всегда были важны, особенно когда в практику начали вводить электронные медицинские карты. С ростом популярности телемедицины сейчас как никогда важно убедиться в том, что ваша медицинская практика понимает и реализует основные правила кибергигиены для защиты данных пациентов и коммерческой информации. Создание культуры киберготовности в вашей практике не только снизит риск взлома, но также лучше подготовит к атакам и предоставит вам нужные инструменты для случаев несанкционированного доступа. Институт киберготовности призывает вас уделять особое внимание человеческому поведению, назначить ответственного сотрудника по киберготовности или «киберкуратора», а также к обучению и повышению осведомленности как вашей лучшей защите и возможности для устойчивости к воздействию извне.

Хакеры используют пробелы в безопасности телемедицины для целенаправленных атак на уязвимые медицинские учреждения. Исследователи обнаружили, что с марта по апрель этого года количество предупреждений о безопасности, отправленных в отделы информационных технологий на 148 хостах самых популярных приложений телемедицины, выросло на 30% по сравнению с тем же периодом годом ранее.

По мере роста популярности телемедицины увеличение количества целевых атак (в том числе рост предупреждений системы безопасности на 117%), попросту вызвано заражением вредоносным ПО.

Когда дело доходит до вопросов телемедицины, наличие прочной основы базовых вещей таких, как пароли, обновления программного обеспечения, фишинг и использование USB, будет неизмеримо полезно, поскольку ваша практика адаптируется к новой «среде телемедицины».

Лучшие практики

Ознакомьтесь с телемедициной, так как она уже не уйдет

- Признайте то, что удобство телемедицины делает ее привлекательной для пациентов.
- Поймите, как чрезвычайные ситуации в области общественного здравоохранения меняют ваши протоколы телемедицины (например, возмещение расходов, межгосударственное лицензирование, правила HIPAA).

Будьте активными, а не реактивными

- Создайте план реагирования на инциденты, отработайте его и предоставьте своим сотрудникам и коллегам [Перейдите на сайт BeCyberReady.com, чтобы узнать, как создать план реагирования на инциденты].

Будьте последовательны с выбранной вами платформой телемедицины на протяжении всей вашей практики

- Узнайте, какие платформы телемедицины соответствуют требованиям HIPAA.
- Расставляйте приоритеты в своих потребностях и проблемах, а также в интересах ваших пациентов при оценке вариантов.
- Обеспечение единообразия и прозрачности.

Изучите основы кибергигиены

- Пароли: включите многофакторную аутентификацию и используйте парольные фразы длиной более 15 символов. Обновления программного обеспечения: включите автоматическое обновление.
- Фишинг: периодически проводите тесты на фишинг и информируйте своих сотрудников о том, как выглядят попытки фишинга.
- USB-накопители: используйте онлайн-обмен файлами вместо USB-накопителей.

Будьте в курсе, будьте подготовлены и будьте киберготовы.

Об Институте киберготовности

Институт киберготовности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов для обмена ресурсами и знаниями, которые используются с целью разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Изучите основы хорошей кибербезопасности с помощью нашего стартового набора или создайте культуру кибербезопасности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше, посетите сайт www.BeCyberReady.com.