SJA SOLUTIONS

HIPAA Compliance: Myths vs. Facts

When it comes to protecting medical practices from security incidents and data breaches, there are a lot of myths and misconceptions floating around. Because the world of medical safety compliance is so vast, we wanted to help clear the air of any confusion. We've compiled a few common myths, and their corresponding facts, to help protect medical practices from the threat of breaches.

Myth: Any indication of compromised data is known as a breach.
Fact: The term "breach" should not be used lightly. Unless it has been confirmed that data has actually been compromised, it is best to use the term "security incident" or "potential breach." Anything that is considered a "confirmed breach" must be reported.

Incidents should be considered a "confirmed breach" when:

- Private health information has been compromised
- Users have gained access to protected health information they should not have access to
- Information has been sent to the wrong person or recipient (this isn't a covered entity)
- Changes were made to private health information without an audit trail
- A workforce member accesses a patient record when it is not necessary for the performance of his/her assigned duties

(These are just a few examples. The team at SJA Solutions can help clarify if something should be labeled an "incident / potential breach" or a "confirmed breach".)

Myth: A security risk assessment only needs to be performed once, and then a practice is set.
Fact: A security risk assessment should be performed at least once a year, if not more, as protocols are always changing and there are new risks arising every day. It is important to compare data year over year and ensure that all correct security measures are in place. A security risk assessment is the first step in protecting a practice against breaches, but implementing proactive security protocols should be an ongoing initiative.

Myth: Breaches only come from outside sources "breaking in" to the system.
Fact: It is actually more common for a breach to come from inside a practice, as opposed to a "hacker." The majority of internal breaches are due to user error (someone discussing a patient's private health information with an unauthorized person, sending a chart to the wrong fax number, etc.) It is important that the entire staff be well-versed and trained on the systems in place and that they understand the specific protocols in place for when an incident does occur.

Myth: The same security requirements apply across the board, no matter the size of the practice.
Fact: Depending on the size of the practice, some rules are required "standards", and some are "addressable." A small practice with a small budget may not be required to use certain monitoring practices if it proves to be too costly.

(SJA Solutions can assess your size, needs, and systems to find out exactly what type of protection you'll need...and what you won't.)

Myth: Mobile Phones require less security than computers.
Fact: With the introduction of "telemedicine", patients and doctors may be lulled into a false sense of security. Phones and portable devices may seem safer since it is rare to hear of a hack on a single phone, as opposed to a large computer system. But, as the trend of Skyping or texting with a doctor grows, it's important that personal devices are kept as safe as office computers.

As long as the device the doctor is using is encrypted and password protected, the doctor can use this to communicate and exchange private information with a patient. But, if that device is stolen or hacked, then it is a serious security issue. In order to avoid a potential breach, practices should be able to prove that they were able to wipe the phone remotely or destroy the private information held on that device.

Myth: Cloud-based medical records are safer and less vulnerable to breaches.
Fact: Cloud-based medical records systems still need extremely tight security. Although cloud users have their own unique usernames and passwords, and the cloud does not live on just one device that can be hacked, it still needs to be treated and monitored as if information were to be living in that system permanently.

Myth: A smaller practice won't be affected by bending the rules. The OCR only pays attention to the larger hospitals.
Fact: The OCR reviews all complaints of HIPAA violations and reports of breaches. Depending on the severity and level of negligence, fines can range from as little as $100 per violation up to $50,000, and in some cases, criminal charges may also be introduced. If over 500 residents of a state have been affected, it is also required for the entity to inform the local media. Between large fines and negative press, a breach could be extremely detrimental to a smaller practice.

Myth: Medical staff are the only ones who are liable for any HIPAA compliance security incidents.
Fact: Anyone who the practice (covered entity) intentionally provides with medical records needs to sign a BAA (Business Associate Agreement). This includes (but is not limited to) a practice's email service provider, cloud based backup services provider, CPA (if billing information has PHI on it), IT Service Provider, or ANY THIRD PARTY that performs a service for the practice that involves the use or disclosure of PHI. While it won't hurt to get one signed, it can hurt not to. If a party doesn't sign and something happens, then the liability falls back on the practice. Don't take any chances.

Myth: Doctor's offices are not allowed to email patients about medical care and health records.
Fact: Doctor's offices can in fact email patients about medical care and health records if the patient chooses to allow that type of communication. If a doctor's office can send an encrypted email to their patients, they do not need permission to do so, they just need an approved email address. Otherwise if a doctor's office doesn't have encrypted email, the practice can sign a release waiver that allows them to send medical-related information to patients via email. Not every practice will do this, but it is worth asking, as it is form of communication that is becoming much more popular in the media field.

If you still have questions or concerns about protecting your medical practice from security threats, you can contact SJA Solutions. Don't wait until there's a problem. Explore the possibilities of a proactive approach to IT.