Insider Threats to Healthcare Data: What You Need to Know and 5 Steps You Can Take Now

Insights
5.21.24

Healthcare data breaches are occurring more frequently and on larger scales than ever before – and while you defend against cyberattacks and other external threats, make sure you do not overlook the critical role your employees play. While many workers have the company's best interest in mind, trusted insiders who have been given access to sensitive health information can cause serious harm by inadvertently or intentionally violating data security and privacy standards. Employers must be prepared for insider threats and take steps to prevent, identify, and address them. We'll give you what you need to know and five steps you should take now.

What's a Healthcare Data Breach and What Laws Apply?

Generally speaking, a healthcare data breach occurs when an individual's sensitive health information – such as their medical records, test results, or personal identification details – are accessed, disclosed, or acquired in an unauthorized way. Healthcare data breaches can implicate a wide range of laws and regulations at state and federal levels. Different rules apply to different entities and vary regarding the type of information protected and what constitutes a breach. This can create a patchwork of compliance obligations for your organization.

One of the biggest and most widely known health data security and privacy laws is the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA applies to covered entities, such as healthcare providers, healthcare clearinghouses, and health plans, as well as certain business associates, which can be individuals or entities that help a covered entity to do its job.

Insider Threats to Healthcare Data

When you think of healthcare data breaches, you might imagine cyberattacks like ransomware and hacking. While guarding your data from cybercriminals and other external threats is extremely important, your defense strategy shouldn't stop there. Healthcare data breaches often are caused – whether intentionally or unintentionally – by your own employees, contractors, or third-party vendors who have authorized access to your sensitive data and systems.

Malicious Insider Threats

A malicious insider makes a conscious decision to act inappropriately and has some motive to benefit themselves or harm your organization. Here are some examples of intentional misuse of health information:

- a departing employee downloading patient data for a possible whistle-blower action;
- an employee using patient information to commit fraud and identity theft or accessing a celebrity's medical records for financial gain; or
- an administrative staff member snooping on medical records for personal reasons.

The financial impact can be staggering. Earlier this year, the U.S. Department of Health and Human Services (HHS) reached a $4.75 million settlement with a non-profit hospital system based in New York City after HHS investigated the hospital for several potential healthcare security violations, which allowed an employee to steal and sell patients' protected health information over a six-month period. The settlement details can be found here.

Unintentional Insider Threats

Insiders can pose a major risk to the health sector even if they do not have malicious intent. Here are some examples of insider threats resulting from lack of training or careless mistakes:

- a residential care staff member casually discussing one patient's mental health issues with another patient who further disseminates that information;
- an employee who falls for a phishing attack that enables bad actors to access your healthcare network;
- an employee leaving an unencrypted laptop unattended, allowing a third-party bad actor to copy sensitive data on the device; or
- remote workers attending sensitive meetings virtually in the vicinity of unauthorized individuals or active voice assistants, leading to data leaks.

What Are the Consequences?

Healthcare data breaches can have serious consequences such as civil and criminal penalties and damage your organization's reputation. For example, HIPAA violations can subject:

- **covered entities and business associates** to civil monetary penalties up to **$68,928** (or up to **$2,067,813** for violations that are not timely corrected) – per incident but subject to annual caps – depending on culpability levels; and
- in severe cases, **individuals** (such as healthcare professionals who knowingly violate HIPAA) to criminal penalties including fines up to **$250,000** and **imprisonment up to 10 years** depending on the nature of the violation.

Your organization should also consider implementing internal disciplinary procedures for employees who violate your healthcare data security and privacy policies – as we'll cover further below.

5 Steps You Should Consider Taking Now

Tackling insider threats should be a joint effort between healthcare leadership and your information technology and human resources departments. Consider taking these five steps:

1. Review and Revise Your HIPAA Policies and Procedures

Make sure to scale and customize your policies for the specific needs of your organization. Because of the huge range in types and sizes of entities that must comply with the HIPAA rules, there is no one-size-fits-all approach – and your approach should be updated as your workforce, operations, and technologies evolve.

2. Train Your Workforce – Thoughtfully and Often

Since insiders are a common cause of breaches and mistakes can be costly, it is imperative that your workforce is aware and current on your HIPAA policies and procedures. Training should be specific to your organization and your employees' job responsibilities, and you should conduct it on a regular basis. Strongly emphasize to your employees that they serve a critical role in protecting privacy and security.

3. Establish a Sanction Policy and Apply It Consistently

You should consider establishing a sanction policy that clearly communicates your expectations for your workforce members, their individual compliance obligations, and the consequences of noncompliance. Doing so can create a culture of compliance, as your workforce members may be more vigilant and less likely to repeat offenses or accidents. And you can eliminate potential claims of discrimination or wrongful termination from employees by pointing to a uniform policy.

Disciplinary action can include warnings, additional required training, and even termination. Last year, HHS issued a newsletter regarding how sanction policies can support HIPAA compliance.

4. Look Out for Warning Signs of Malicious Insiders

Certain indicators can raise red flags of nefarious activity, including:

- official **records** of security violations or crimes;
- unprofessional or combative **behavior**; and
- suspicious **activity** such as creating backdoor accounts, password changes that deny others access to the data, massive downloads of corporate data, or sending sensitive data to a non-work

access to the data, massive downloads of corporate data, or sending sensitive data to a non-work email address.

By detecting potential insider threats, you may be able to prevent or reduce harm to your organization.

5. Don't Forget About Other Laws Beyond HIPAA

Healthcare data breaches can bring other laws into play, including:

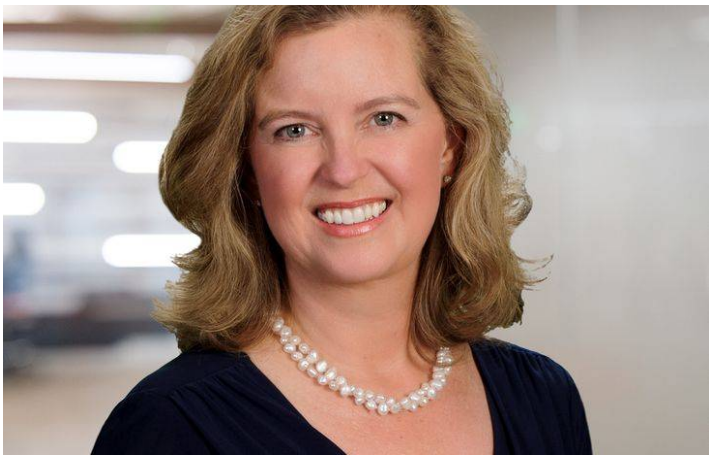
- the federal Health Information Technology for Economic and Clinical Health Act, which strengthened HIPAA's privacy and security provisions;
- the **Federal Trade Commission Act**, which prohibits companies from misleading consumers about what is happening with their health information and provides similar breach notification rules as HIPAA that apply to vendors of personal health records and their third-party service providers; and
- **other federal laws** that require employers to keep employee information confidential – such as disability-related medical information under the Americans with Disabilities Act or genetic information under the Genetic Information Nondiscrimination Act;
- **state consumer health data protections**, which can be enforced by State Attorneys General and we previously covered here;
- **state breach notification laws**, which may impose stricter timing requirements than HIPAA for providing the breach notification; and
- **private lawsuits,** which have permitted individuals in some states to bring claims against covered entities for alleged HIPAA violations, even though that law does not provide any private right to sue.

You should work with your legal counsel to ensure compliance with all applicable laws and how to incorporate compliance obligations beyond HIPAA into your policies, procedures, and training programs.

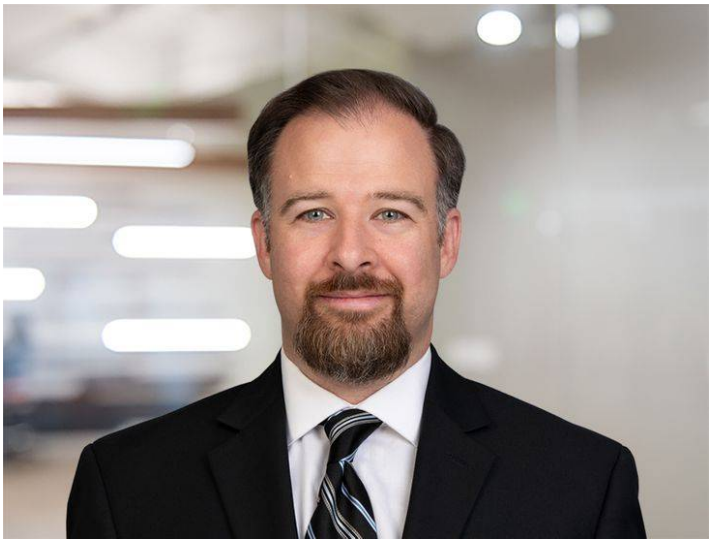
Conclusion

If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, any attorney on our Healthcare Industry Team, or any attorney on our Privacy and Cyber Team for more information. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information on this and other employment topics directly to your inbox.

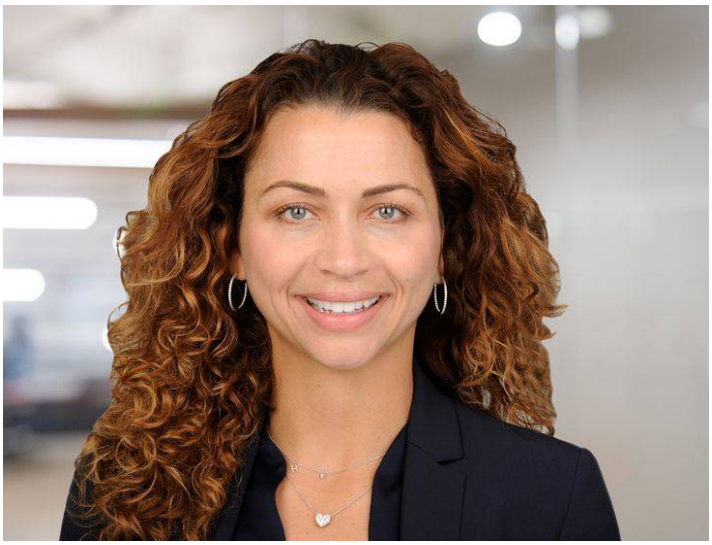
Related People



Lorie Maring
Partner
404.240.4225
Email



Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email



Hannah Sweiss

Partner
818.230.4255
Email

Service Focus

Privacy and Cyber

Industry Focus

Healthcare