WHITE PAPER

Effective Healthcare Data Breach Response

How Not to Panic When Sensitive Data is Compromised

Healthcare IT is undergoing a complex and challenging (but necessary) transformation. Today, healthcare organizations must not only keep up with ever-changing regional and global regulations surrounding protected health information (PHI). They must also stay one step ahead of cybercriminals and situations — even if they're accidental — that could lead to data breaches. Adding to the complexity, is the trend toward mobile devices and mobile patient care; if a portable device is lost or stolen, the consequences could be devastating to both the patients and the healthcare provider.

Several studies have concluded how medical records fetch higher prices than credit card data on the Dark Web, and the value of PHI is only rising. Medical data can be used to buy drugs or equipment that can be resold, and it can be used to make false insurance claims. In 2017, Ponemon Institute reported the cost for healthcare providers hit an all-time high of $7.35 million for a data breach. Because medical data is so valuable, even the FBI has warned healthcare providers that cybercriminals are targeting healthcare providers more than any other industry. The costs and consequences of a data breach could cripple a healthcare organization, especially if the organization does not respond quickly.

Whether a device is lost or stolen, breached with malicious intent, or hijacked because of poor endpoint hygiene, healthcare providers may be compelled to notify authorities of a breach. Depending on the circumstance, region, and type of data at risk, the provider must notify the individuals whose PHI was compromised, the U.S. Department of Health and Human Services, and sometimes even the media in an attempt to contain the story. Data breach consequences may also include audits, Office of Civil Rights (OCR) investigations, penalties, class-action lawsuits, as well as the accompanying loss of trust and prestige in the healthcare community. How a healthcare provider responds to a data breach can be the difference between a simple security incident and long-term reputation and financial damage.

SIX STEPS TO EFFECTIVE DATA BREACH RESPONSE

1. ACTIVATE YOUR RESPONSE PLAN OF ACTION

The team responsible for post-breach triage must reach out to the crisis management team as soon as a security incident is discovered. The crisis management team should be comprised of a cross-section of people including legal, PR, internal communications, IT, and leadership. Ideally, this team will have participated in role-playing and other exercises so they can immediately respond rather than trying to build their plan in the midst of an incident. When properly prepared, this team can greatly improve response time and reduce financial and reputational risks.

Once the team is engaged, they can identify required internal and external communications about the breach. It's important to tailor the response to the specific situation, customer demographic, level of risk and compliance requirements.

2. LIMIT THE DAMAGE

Decide on the severity of the breach and perform remote security actions, such as deleting sensitive data from the device. It is a good idea to also produce proof as to when data was last accessed on a device. If data access did not occur between the time of the security incident and when the data was deleted, it may be possible to avoid filing a breach report.

Determine the facts of the breach. Identify ownership of audit reports, post-event actions, and findings. This type of information will help dictate the appropriate post-breach course to follow.

3. UNDERSTAND THE REGULATIONS

Assuming the appropriate pre-breach efforts have been taken, ensure that post-breach the most current iterations of breach notification laws, such as HITECH, HIPAA and Gramm-Leach-Bliley Act are adhered to. Note that local breach notification laws can be more stringent than federal law, so keep up-to-date on local data breach notification laws.

Determine who needs to be notified about the breach, and through what channels. If the device is encrypted by methods approved by the National Institute of Standards and Technology (NIST), an exemption (Safe Harbor) may be claimed from the HITECH Act breach notification requirements. Even if it is not required by law to contact patients, consider the risk to patients and your reputation if a notification is not done properly and the breach is made public by other means.

4. COLLECT, DOCUMENT AND ANALYZE EVIDENCE

As soon as the breach is discovered, it's critical to begin documenting, analyzing and preserving evidence to be able to support the burden of proof to regulatory agencies. Under current law, risk assessment must demonstrate that due diligence was completed with consistent and defensible methodologies. Start by recording the date and time the breach was noted and establish the device's chain of custody.

5. DETERMINE THE EXTENT OF THE DAMAGE

In the early stages of a security incident, it's important to determine if the potential breach was accidental or malicious. Identifying who was affected, as well as the quantity and data types that were accessed will help to determine the level of exposure.

A breach is defined as 'an impermissible use or disclosure of protected health information' by an entity other than a business associate[1]. Depending on the region, PHI may include name, social security number, medical information, and financial account numbers with security codes or passwords.

It may not be classified as a notifiable breach if an organization can illustrate that encryption was in place at the time the device went missing, and that PHI was not compromised. Run encryption status reports and note the last accessed date of sensitive files. If encryption was in place and files were not accessed, the risk of a data breach is minimized, and the organization can potentially avoid filing a breach report.

6.SEND COMPLIANT NOTIFICATIONS

If required to send data breach notifications, determine the channels through which patient, regulatory, and media notifications will be sent[2]. Notifications should include details of the breach, how it was responded to, the status of the investigation and information about identity monitoring and protection services offered to those affected[3]. All communications should have consistent wording and should be approved by legal counsel.

1 HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

2 The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

3 List of applicable forms and additional information

CONCLUSION

Establish a ‘culture of cybersecurity’ at your facility. The best programs start at the top (i.e., the board of directors, C-suite, upper management, etc.). Buy-in is also required across the organization. The Department of Health and Human Services provides tips on cybersecurity.

MINIMIZING DATA BREACH DAMAGE WITH PERSISTENCE® TECHNOLOGY

Persistence technology by Absolute ensures that portable devices are secure regardless of location or user. This technology is embedded in the core of devices at the factory. Once the Absolute software agent is installed and activated, Persistence ensures that the agent remains intact.

If the agent is damaged or missing, Persistence triggers an automatic reinstallation the next time the device connects to the internet — even if the hard drive is replaced, the firmware is flashed, or the device is wiped clean to factory settings. This ensures that IT can maintain a constant connection and secure the device and any PHI it contains.

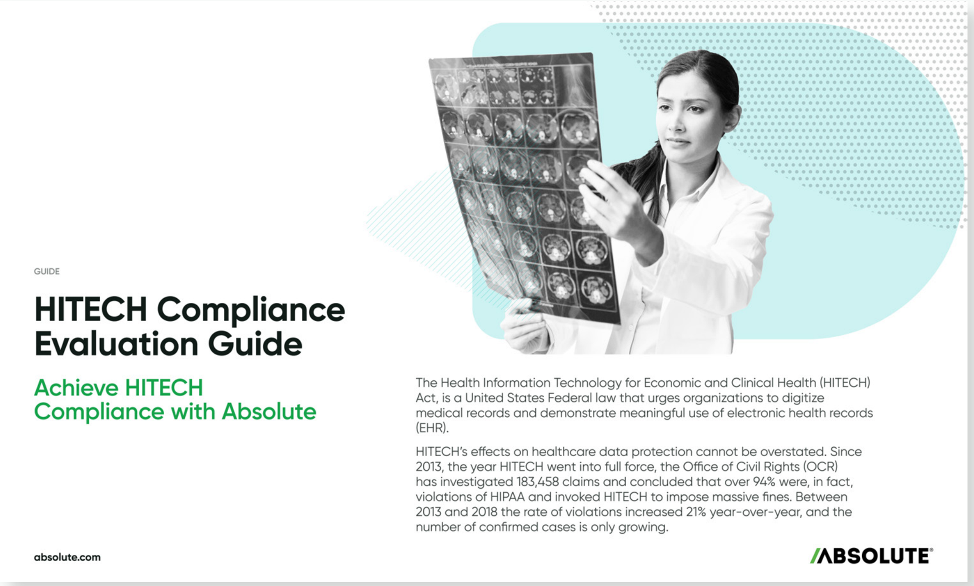
While healthcare organizations must support a mobile workforce, they must also ensure and prove that PHI is secure and that they are in compliance at all times. Technology solutions that help IT enable staff mobility while mitigating the risks of data breaches, are critical to quality patient care and the success of the organization.

Absolute can help maintain regulatory compliance by providing proof that encryption or other security measures were in place at the time a security incident occurred. By reporting on the status of the data on the device, Persistence technology enables organizations to identify if data was accessed post-breach, and whether a breach notification must occur.

Tailored specifically for healthcare organizations, Absolute for Healthcare provides a full complement of features and remote capabilities so that you can control and secure healthcare data and devices. The solution includes the support of certified Healthcare Information Security and Privacy Practitioners (HCISPP) and ASIS-Certified Protection Professionals (CPP) on the Absolute Investigations team to help you identify when, and if, a breach notification should occur. For more information about Absolute solutions for Healthcare, please visit:
absolute.com/healthcare

REFERENCES

- Forrester: Healthcare Must Embrace Zero Trust to Address PHI Vulnerabilities
- Centers for Medicare & Medicaid Services: Health Care Fraud and Abuse
- Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview
- Exclusive: FBI warns healthcare sector vulnerable to cyber attacks
- HealthIT Security: Healthcare Hacking Leading Cause of 2017 Incidents
- HealthIT Security: 16.6M Affected by Healthcare Data Breaches
- Gartner: Healthcare Provider CIOs Must Translate Information Into Action by Controlling Patient Data
- Gartner: Five Best Practices that Healthcare Provider CIOs Can Use to Reduce Mobile Device Security Risk
- Quick-Response Checklist from the HHS, Office for Civil Rights



GUIDE

HITECH Compliance Evaluation Guide

Achieve HITECH Compliance with Absolute

The Health Information Technology for Economic and Clinical Health (HITECH) Act, is a United States Federal law that urges organizations to digitize medical records and demonstrate meaningful use of electronic health records (EHR).

HITECH's effects on healthcare data protection cannot be overstated. Since 2013, the year HITECH went into full force, the Office of Civil Rights (OCR) has investigated 183,458 claims and concluded that over 94% were, in fact, violations of HIPAA and invoked HITECH to impose massive fines. Between 2013 and 2018 the rate of violations increased 21% year-over-year, and the number of confirmed cases is only growing.

absolute.com

/ABSOLUTE®

Ensure HITECH Compliance

Identify the required elements to achieve HITECH compliance with the Absolute platform guide.

Get the Evaluation Guide

ABSOLUTE®

Absolute Software makes security **work**. We empower mission-critical performance with advanced cyber resilience. Embedded in more than 600 million devices, our cyber resilience platform delivers endpoint-to-network access security coverage, ensures automated security compliance, and enables operational continuity. Nearly 21,000 global customers trust Absolute to protect enterprise assets, fortify security and business applications, and provide a frictionless, always-on user experience.

Request a Demo