INDUSTRY WHITEPAPER

# Preparing your organization for the inevitable **HIPAA Audit**

A four step guide to protecting your organization's reputation and your customers' data

egress®

In their day-to-day role, healthcare organizations have to process enormous amounts of data, most of which is highly sensitive and requires security in order to protect it.

This includes both Protected Health Information (PHI) and sensitive personal information, such as social security numbers and financial data. As more and more of this information goes digital and needs to be communicated electronically, it is critical that healthcare providers maintain the levels of privacy and security their patients have come to expect. A primary aspect of this is ensuring compliance with the Health Insurance Portability and Accountability Act (HIPPA).

## HIPAA compliance – the benefits

By embracing HIPAA compliance, organizations not only avoid the expensive fines and reputational damage of a high-profile data breach, but also see tangible improvements in patient care. To ensure compliance, healthcare providers are forced to invest in the necessary technology, processes and training to protect sensitive information. What's more, this investment also has the added benefit of enhancing connectivity and communication between staff, patients and external partners.

# Is there a disconnect between compliance and data breach prevention?

## Failure to comply – the risks

In October 2015, the Office for Civil Rights (OCR) decided to introduce Phase 2 of the HIPAA Audit Program, which was officially announced earlier this year. This was a game changer for the healthcare industry. It started with the U.S. Department of Health & Human Services (HHS) criticising the OCR, stating: "The OCR should strengthen its oversight of covered entities." It resulted with all organizations handling PHI anticipating increased scrutiny and potential auditing ahead of, or as a direct result of, a data breach.

The rules are pretty clear: if your business has a breach involving 500+ individuals, the OCR will require:

- All company policies and procedures relating to the security of PHI
- A risk analysis report, demonstrating:
  - What you did to mitigate the risk
  - What you are doing to prevent a breach in the future

So what are the consequences should an organization have a breach and fail the accompanying audit? The answer:

- A substantial fine
- Reputation damage, which includes listing on the HHS website: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Potential legal action
- Loss of patient confidence

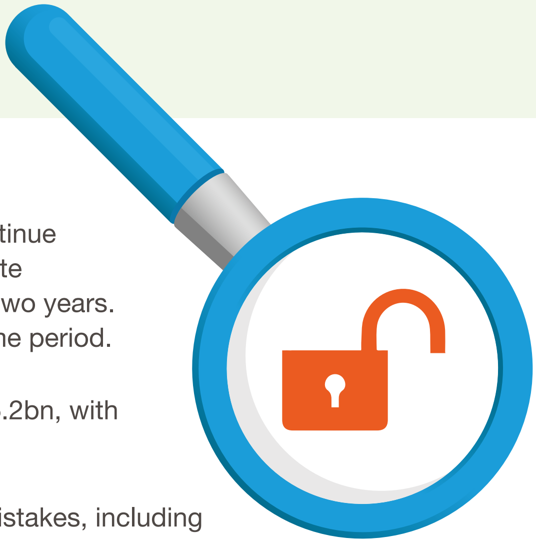
> "The cost of data breaches to the industry currently stands at $6.2bn, with the average cost now sitting at $2.2m."

## The research doesn't lie

As research demonstrates, data breaches in US healthcare continue to rise. Recent statistics by ID Experts and the Ponemon Institute show 90% of providers have suffered a data breach in the last two years. Of these, 45% suffered more than five data breaches in the same period.

The cost of data breaches to the industry currently stands at $6.2bn, with the average cost now sitting at $2.2m.

Of these breaches, approximately 50% were down to insider mistakes, including employee error, data accidentally lost, and data sent to the wrong recipient.



# How can healthcare providers protect themselves and their patients?

With data breaches on the rise and the ensuing HIPAA Audits becoming more stringent, organizations need to move quickly to ensure they are compliant.

In most cases, healthcare providers need to consider a four step approach:

## 1. Planning

In many cases, organizations are under such pressure to act that planning is overlooked in favour of investment in new systems and processes intended to mitigate the risks of a data breach. As a result, organizations end up with badly implemented processes, and systems sitting in silo that are hard to use and sit outside an end-user's day-to-day work practices.

Instead, healthcare providers need to first consider their people and processes, and then the best-fit technology solution (if appropriate). In most cases, by limiting the changes to current processes, and implementing technology that is easy to use and integrates into an existing set of infrastructure, organizations have the best chance of successfully managing the transition to new working practises.

## 2. People

For any change in process or technology to be successful, an organization needs its people to understand and embrace the importance of data security.

Education therefore plays a key role in any organization's move towards maintaining HIPAA compliance. In most cases, staff will immediately recognize the importance of security when sharing sensitive data, but will often be unsure of how to identify information that needs to be secure versus data that doesn't, and the associated process for securing it.

> By putting in place simple processes, easy-to-use technology and the underlying training, an organization can ensure its people are its first line of defence rather than its biggest vulnerability.

At the same time, providers should consider data security solutions that take decision-making away from the end-user. For example, email and file classification can be implemented as part of a Data Loss Prevention (DLP) solution to integrate with email and file encryption. Consequently, an organization can put in place policy that decides whether an email or a document should be secured (encrypted) at the gateway, rather than relying on a member of staff to remember to encrypt before sending from their desktop.

## 3. Technology

One very obvious way to help protect your organization against a data breach and work towards HIPAA compliance is to implement data security technology.

The OCR themselves state that the use of encryption should be a mandatory requirement when protecting PHI.

As part of any investment in technology, the following should be considered:

a. **Ease of use** – if data security solutions are difficult to use or require considerable investment in training, users will typically revert back to older, less secure methods for sharing data – often via clear text email.

b. **Integration** – the more data security technology can integrate into existing infrastructure, the greater the usage levels. This is particularly important given the shift towards the Cloud and mobile working practises. For example, an organization moving to Microsoft 365 needs to know that their choice of email encryption solution or secure large file transfer mechanism will seamlessly integrate into a hosted Exchange environment. Similarly, when staff are constantly on the road, secure and easy access to encrypted data via mobile devices is equally important.

c. **Protect data throughout its lifecycle** – no longer can secure information sharing be treated in silo. From the point of creation, to sharing it internally with colleagues or externally with patients and partners, PHI needs the appropriate levels of protection and care applied to it. As a result, organizations need to consider how they combine / integrate secure data exchange mechanisms – such as email encryption, large file transfer and secure online collaboration – with classification, DLP, auditing and reporting. Only by treating data security with this holistic approach will healthcare providers be able to mitigate the risk of a breach and demonstrate the necessary levels of HIPAA compliance.

## 4. Auditing and reporting

HIPAA audits are now a reality for all healthcare providers. As part of an audit, the OCR will want to understand:

- Where PHI data is being transmitted
- How it is being transmitted (email, large file or collaborative environment)
- Who had access to the data
- Where the data is stored at rest and in transit

In order to achieve this level of reporting, an organization is going to need sophisticated auditing technology in place that tracks data sharing at all times and can provide detailed and accurate reports within a short timeframe. Reliance on multiple reporting tools that are separate from one another limits both the effectiveness of any auditing and speed of response.

> “Reliance on multiple reporting tools that are separate from one another limits both the effectiveness of any auditing and speed of response.”

Not only is this technology instrumental in HIPPAA compliance, but organisations can also benefit more generally from monitoring how PHI is shared in order to enhance processes and policies that will in turn limit future data breaches.

### About Egress Software Technologies Inc

Egress Software Technologies is the leading provider of data security services designed to protect shared information throughout its lifecycle.

Utilizing AES 256-bit FIPS 140-2 approved encryption, the Egress Switch platform provides the highest level of security for complete end-to-end data exchange. In the U.S., Switch helps organizations remain compliant with industry and government standards and regulations designed to safeguard sensitive consumer data, including HIPAA and the GLBA.

The award-winning Switch portfolio of products includes email and document classification, email and file encryption, secure managed file transfer, secure online collaboration and secure email and file archiving. The platform offers a seamless user experience, powerful real-time auditing and patented information rights management, all accessible using a single global identity.

**www.egress.com**

✉ info@egress.com
☎ 1-888-505-8318
@EgressSwitch

egress®