E-book

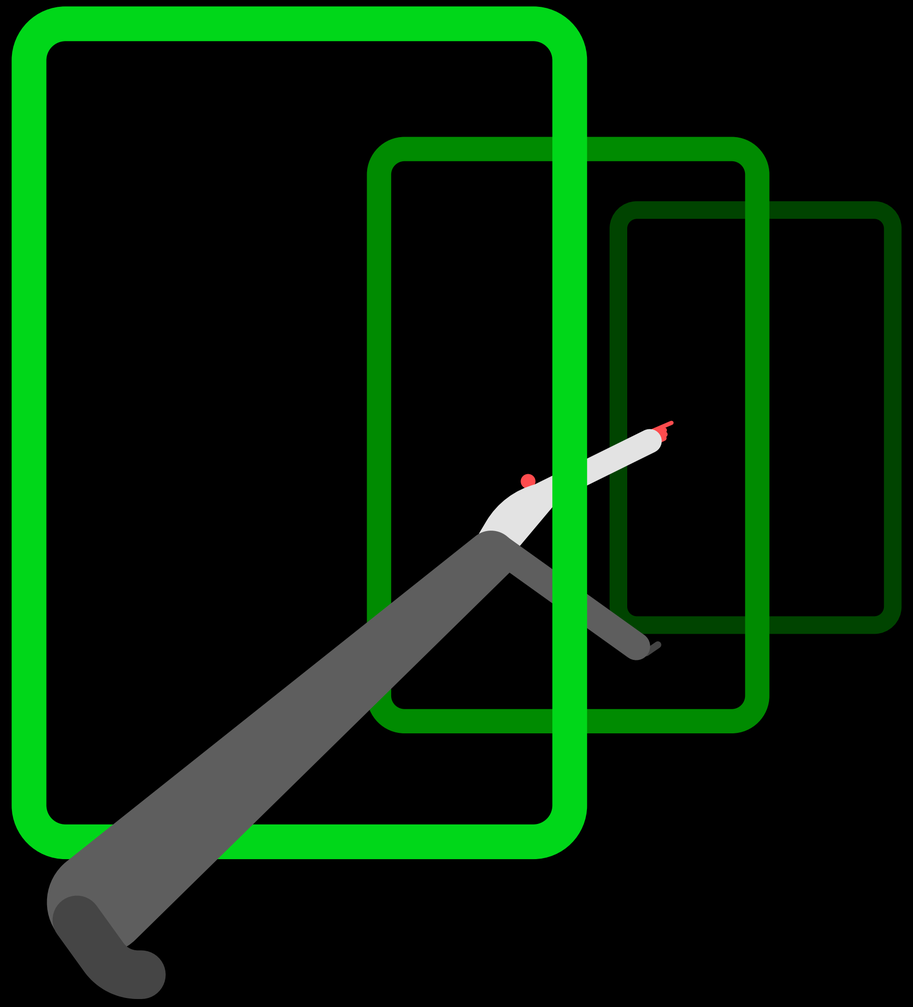
HIPAA Compliance and Financials: What to Look for and What's Next

Healthcare

Sage

DSD BUSINESS SYSTEMS

Table of contents



Introduction

When the Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996, its purpose was to improve the portability and accountability of health insurance coverage for employees between jobs.

Since then, the scope of HIPAA has grown significantly. HIPAA became a vehicle to encourage healthcare providers and other covered entities to move to electronic healthcare records and, in turn, keep that patient data secure.

Healthcare organizations take HIPAA compliance very seriously, but the inherent complexity of this law and its regulations makes maintaining compliance across all systems challenging.

Let’s look at some of the hidden dangers to watch for in HIPAA compliance.

Sage DSD BUSINESS SYSTEMS

Protected health information

Defining protected health information
Protected health information (PHI) is individually identifiable information that's held by a covered entity and that relates to the past, present, or future of someone's health, healthcare, or payment of healthcare and includes demographic information.

The complex definition is reflective of this complex environment. PHI can relate to treatment or payment for health care. Here are some examples of both:

Patient information
✓ Medical Records
✓ Images
✓ Prescriptions

Payment information
✓ Names
✓ Addresses
✓ Phone numbers
✓ Medical record numbers
✓ Billing information

Why is PHI so valuable to bad actors?
Criminals intent on committing fraud hold onto health information for a long time.

Information like age, demographic, and location can be used to estimate what medical conditions someone might have, in order to perpetrate a false billing scheme.

Because of this, on the dark web, PHI collects as much as 20x the amount of money as credit card information

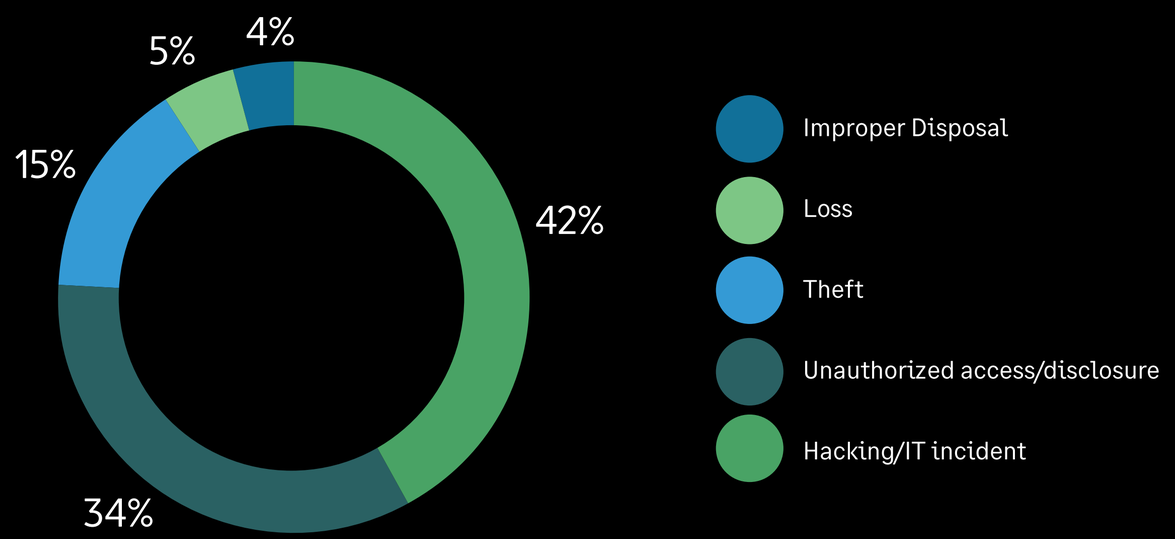
HIPAA breaches

Top causes of healthcare data breaches
In 2017, hacking accelerated as the number one cause of PHI data breaches.

Unauthorized access and disclosure is the second-leading cause of HIPAA breaches. This typically comes from insider threats. This could come in the form of misdirected communications, misconfigured internal systems, employee access of PHI outside of their duties, etc. According to the U.S. Department of Health & Human Services, insider threats are becoming one of the largest threats to organizations.

If a breach does occur, experts agree that a fast resolution is key to reducing the severity of the consequence.

Data breaches leading to HIPAA violations came from a variety of sources.



Source: U.S. Dept. of Health & Human Services, Office of Civil Rights, Report to Congress 2015-2017

Consequences of a data breach

Potential HIPAA violation penalties

1. **Civil monetary penalties** are imposed per violation and can be substantial, resulting in the loss of millions of dollars.
2. **Criminal penalties** occur when a person knowingly obtains or discloses PHI and can result in prison time in egregious cases.
3. **Class action lawsuits** are increasing in number, based on state privacy or negligence laws.
4. **Direct costs** include the cost of investigation, notification, and mitigation of the impact of the breach.
5. **Indirect costs** capture damage to reputation and increase of churn. Healthcare organizations experience a greater impact than any other industry in unexpected and unplanned loss of customers after a data breach.*

*The Ponemon Institute/IBM Security, 2019 Cost of a Data Breach Report

Risk prevention

It is essential to take steps to prevent a breach of PHI before it occurs. Having a plan in place in the event of a breach can prepare your organization for a swift resolution, therefore reducing the cost. The Office of Civil Rights (OCR) expects that healthcare organizations strive for full compliance.

Prevention checklist

- ☐ Perform a **security risk analysis** and resolve identified risks
- ☐ Develop written **policies, procedures, and standards of conduct**
- ☐ Employ a **compliance officer** and compliance committee
- ☐ Design and implement effective **training and education** for staff
- ☐ Prominently display **disciplinary guidelines** and enforce standards
- ☐ Execute **continuous monitoring and auditing** internally
- ☐ Implement, review, and revise **business associate agreements**

How to mitigate costs in the event of a breach

Early detection can significantly reduce the cost of a data breach.*

The earlier you catch a breach, the lower the cost to the organization. If a breach does occur, use tools to facilitate its prompt detection. Be sure to have an incident response team in place to execute your response plan and strategy.

Implement effective lines of communication internally and with partners, media, patients, and regulators.

Business Associate Agreements (BAA) are essential to protecting your organization and to HIPAA compliance. If you want to do business with a company that refuses to sign a BAA, look elsewhere.

*The Ponemon Institute, 2017 Cost of a Data Breach Report

Sage DSD BUSINESS SYSTEMS

HIPAA-compliant financials

How Sage Intacct can help
When you think about HIPAA compliance, your financial management system might not immediately come to mind.

Keeping your PHI protected means protecting all of it—included PHI in your financial management system. Examples of this include issuing a refund to a patient, accounting for additional services (i.e. clothing or housing allowances) to patients, or providing payments to caregivers.

HIPAA is flexible and scalable—there is no such thing as an organization too small to be HIPAA compliant. Treat your PHI with the same concern as you would treat a patient and encourage that culture no matter your size. Smaller organizations are sometimes targeted by hackers, who assume security may not be a priority.

The Sage Intacct Advanced Audit Trail can help you on your path toward full compliance. Sage Intacct will sign a Business Associate Agreement to formalize its commitments around HIPAA and is Avertium (formally Sword & Shield) certified for HIPAA compliance.

Sage DSD BUSINESS SYSTEMS

A look ahead

What's next with HIPAA?
As the healthcare industry undergoes significant change, HIPAA will evolve, as well. We're seeing industry trends that may affect HIPAA and data privacy in the coming years.

In the United States, we've historically seen verticalized privacy laws to protect data, such as in healthcare, children's affairs, and finance.

Europe, however, has taken a different approach with broader data protection laws (like GDPR). We are starting to see the United States take steps in that direction (as is the case with the California Consumer Privacy Act). In addition, other state-level laws are providing a baseline set of data breach rules that applies to all different types of protected information. This could be an area of significant development both legislatively and compliance-related in the coming years.

Also, changes could be coming as regulators look at how healthcare organizations share data amongst themselves and with third parties and how patients can access and share their own protected health information.

Sage DSD BUSINESS SYSTEMS

Takeaways

Sage Intacct delivers HIPAAcompliant healthcare cloud accounting software
Even if your organization doesn't require a HIPAA-compliant financial system today, you may need one in the future. To learn more about our HIPAA guidelines, visit sageintacct.com/HIPPA-guidelines.

Sage Intacct
Sage Intacct is the #1 cloud financial management system for data-driven, growing healthcare organizations. Our security safeguards have been certified as HIPAA- and HITECH-compliant by Avertium (formerly Sword & Shield), and Sage Intacct is the only accounting software endorsed by the AICPA.

Data Sheet

HIPAA: Safeguard Protected Health Information

Read Now

Sage DSD BUSINESS SYSTEMS

Sage

DSD
BUSINESS SYSTEMS

800-627-9032

www.dsdinc.com

info@dsdinc.com