sage Intacct

WHITEPAPER

New Research: Finance Professionals and PHI

Financial systems may be putting non-acute providers at risk for HIPAA violations

Healthcare

Contents

Introduction

Sage Intacct recently retained Porter Research to conduct a market study targeting financial and executive leadership within non-acute facilities, including ambulatory groups, radiology groups, surgery centers and skilled nursing facilities, to better gauge their understanding of Protected Health Information (PHI) and HIPAA compliance as it relates to finance and accounting professionals in their organizations.

The study revealed that while most respondents agreed that protecting patient PHI was important, they fail to recognize that a significant portion of their daily responsibilities requires their financial staff to access PHI – resulting in an increased risk of exposure, data breaches and ultimately HIPAA violations.

In addition, the study showed that most respondents rely heavily on written policies and employee education as the primary means for avoiding HIPAA violations. This, however, leaves room for human error, which can be minimized in the finance and accounting departments with the implementation of modern HIPAA-compliant financial management systems.

This paper reveals five major findings from the research that will help financial leaders better understand their risks when it comes to HIPAA violations in their own departments and gives practical advice on how to mitigate these risks going forward.

Understanding PHI in a finance setting

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 as the healthcare industry has moved decisively toward electronic healthcare records (EHR) systems where terabytes of data reside in the cloud instead of paper-based file folders. In addition, the increased pressure of value-based care reimbursement models has dramatically extended the use of clinical patient data across the enterprise. And as the threat of both internal and external data breaches continues to soar, all types of healthcare organizations are feeling the pressure to protect their data.

Financial and business leaders within non-acute care providers must become more aware of these changing dynamics and risks associated with protecting their patients' PHI.

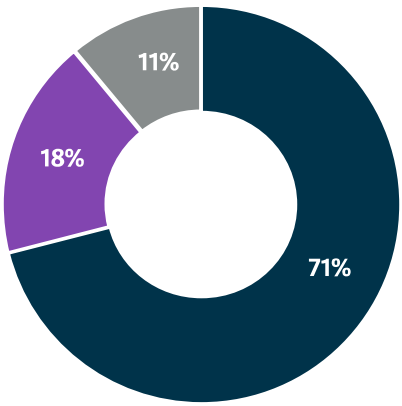
Five key findings from the market research

#1: PHI and HIPAA are misunderstood by many non-acute care financial teams.

Healthcare organizations take HIPAA compliance very seriously, but the inherent complexity of this law and its regulations makes maintaining compliance across all systems challenging. The introduction of new waivers by the ONC in response to the global pandemic has further complicated the industry's understanding of when they can share what information with whom.

And when it comes to finance and accounting professionals, there is a significant gap in understanding PHI, as evidenced by the recent Porter Research study. While most respondents understood that medical records, images and prescriptions were PHI, fewer realized that names, addresses, account numbers, billing information and dates directly related to an individual patient can also be considered PHI.

The vast majority (71%) claimed that their financial management systems did not use PHI, when in fact many of the more common actions performed daily, such as issuing patient refunds or ensuring proper billing for the patient portion, require financial personnel to access PHI. Non-acute providers must be aware of and protect PHI as it comes into their financial systems.



Does your organization have PHI in your financial management system?

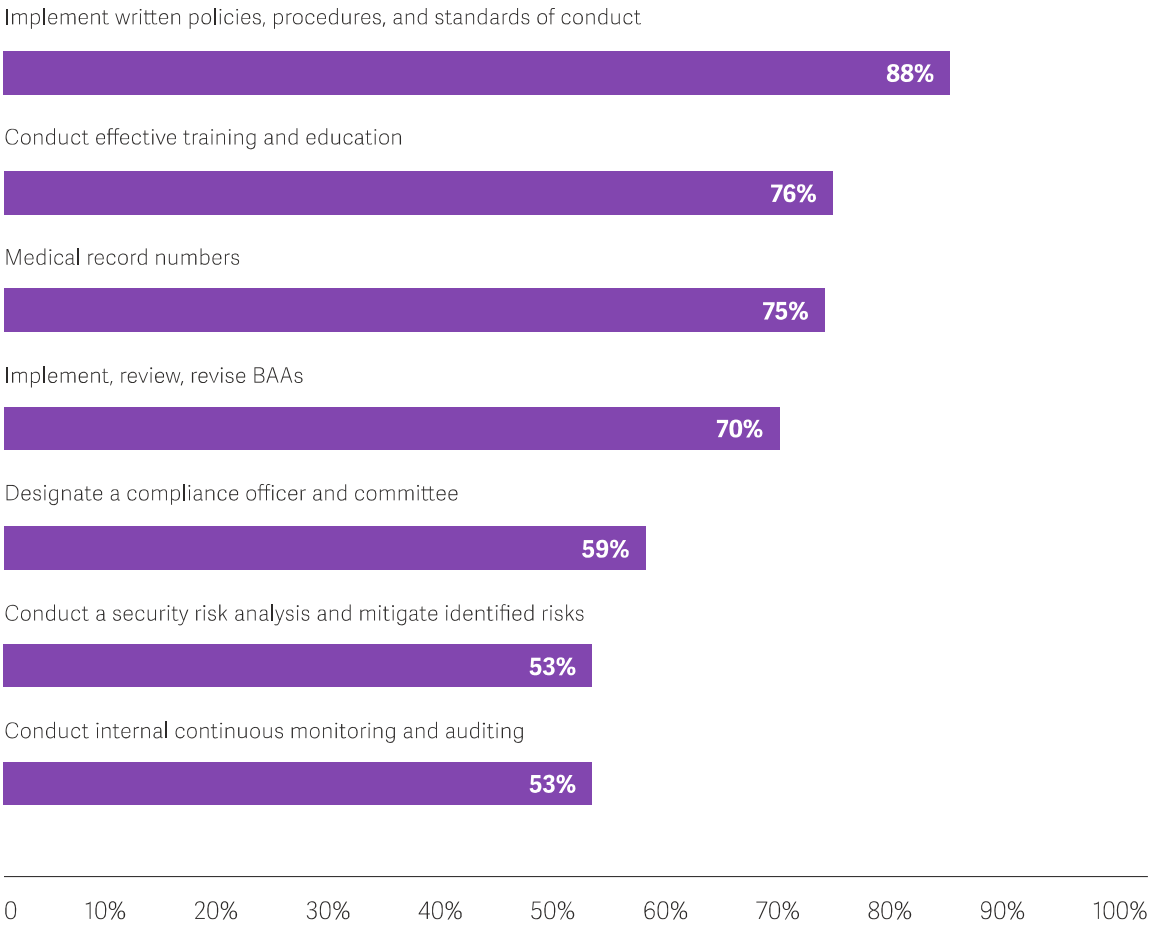
- No
- Yes
- Unsure

#2: Many non-acute organizations are relying primarily on written policies for compliance

82% of non-acute organizations surveyed reported that they have policies in place to prevent a data breach. In fact, the most common methods used for preventing PHI breaches are written policies/standards of conduct, staff training/education and use of medical record numbers. While these methods are needed and, if implemented properly, effective, they also may leave room for human error.

It is important for care providers to utilize modern technology within their financial management systems that can not only help enforce the written policies through automated workflows, but also capture insights into what data was viewed or touched, when and by whom. This type of intelligence can be vital when it comes to investigations and audits by telling which data elements have been exposed to whom. Non-acute facilities should leverage available HIPAA compliant financial management software solutions.

Which of the following does your organization employ to prevent breaches of PHI?



#3: Financial functions will continue to require greater access to clinical and PHI data in the future

As the lines between clinical and financial performance begin to blur even more under value-based care contracts, financial and accounting teams will need greater access to clinical and patient data. For example, direct contracting is an advanced alternative payment model that aims to reduce expenditures and allow patients, employers, or clinicians to communicate directly to pay out-of-pocket for some or all medical services provided by a practice. This is the model that Sage Intacct customer Vera Whole Health employs. In order to be successful in this model, you must be able to understand the success or failure of your value-based contracts. Practices must be able to see the clinical, financial and operational data in real-time to understand the whole operation.

In addition to supporting value-based care initiatives, access to PHI is required to perform many of the daily functions for finance and accounting professionals. For example, 47% of respondents use their financial management systems to issue refunds to patients. Other functions related to ensuring proper patient billing, patient collections and remittance processing may also require access to PHI.

The more data that is being used to demonstrate and analyze patient outcomes and to support performance-based measures, the more opportunities there are for HIPAA violations to occur within financial teams and systems. Non-acute facility leaders must consider all traditional and emerging financial responsibilities when attempting to prevent HIPAA violations.

Sage Intacct's Advanced Audit Trail has been certified as HIPAA- and HITECH-compliant by Avertium and will enter into a Business Associate Agreement.

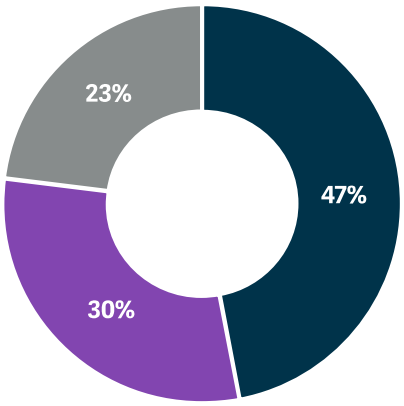
#4: Growing internal threats must be considered as important as external threats for data breaches.

Among survey respondents, most were familiar with the traditional external threats of things like cybersecurity breaches, when an external threat gains access to the systems. But far fewer respondents were aware of the internal threats, such as when employees access PHI outside of their duties or improperly dispose of PHI. According to the US Department of Health and Human Services, insider threats are becoming one of the largest threats to organizations. Non-acute facilities must implement systems that help neutralize these insider threats and create data-access audit trails as the daily work is being performed across the organization, including the financial and accounting functions.

#5: Consequences for HIPAA violations are well understood, but most organizations are not properly prepared.

While most organizations reported a solid understanding of the consequences associated with HIPAA violations, such as damaged reputations in their communities, increased churn in patients and monetary penalties, few reported awareness of additional hardships such as Class Action Lawsuits and the direct costs associated with the investigation, notification of patients and mitigation of the cause of the breach.

In addition, nearly 50% of respondents reported that they do not currently have incident response teams in place in the event of a data breach. Financial leaders of non-acute organizations should be included in any incident response planning efforts to ensure they are aware of what their organizations should do in the event of a breach.

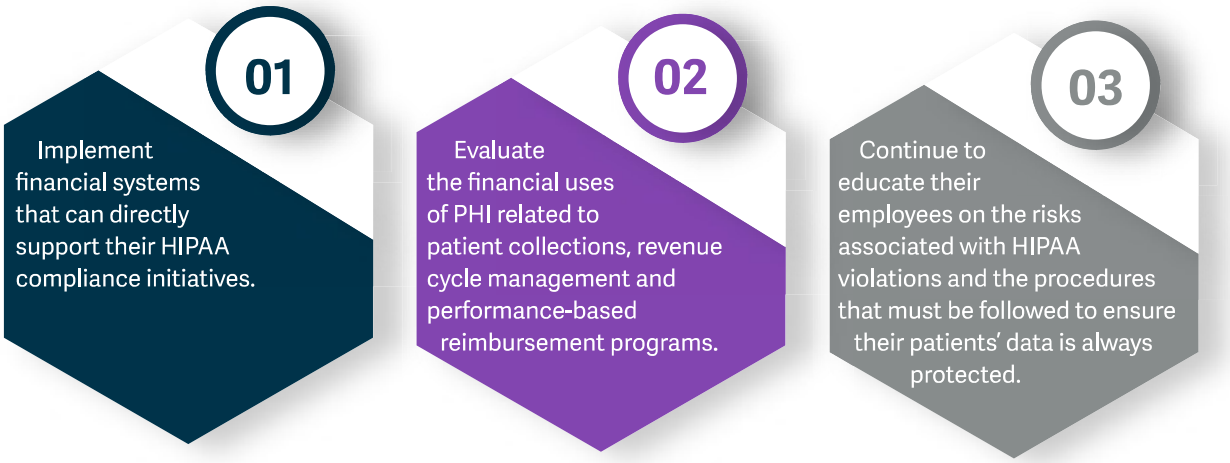


Does your organization have an incident response team in place in the event of a data breach?

- No
- Yes
- Unsure

How to properly prepare your financial organization

Since the inception of HIPAA nearly 25 years ago, healthcare providers of all types have taken great steps to protect patient data. However, as the volume of data increases exponentially, and the uses of that data continue to expand across organizations – including the financial teams – providers must take a closer look at how to better support their ongoing compliance efforts.

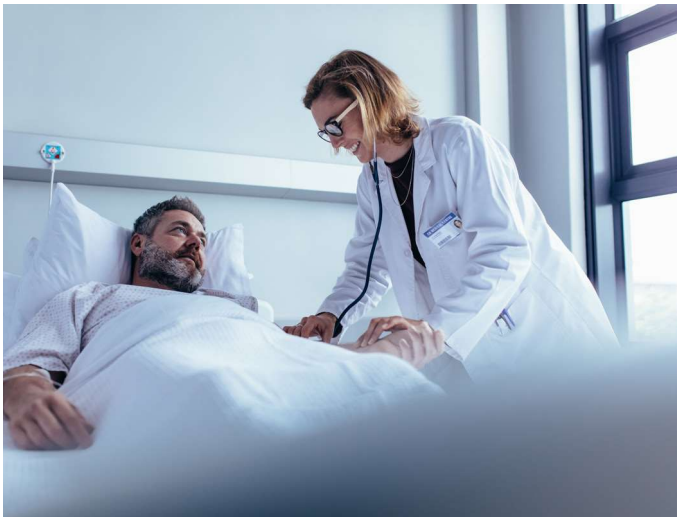


To learn more about HIPAA compliance and how non-acute care providers are using technology to help maintain HIPAA compliance in their financial management systems, visit: **https://www.sageintacct.com/healthcare-accounting-software**

About 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.

Our modern, true cloud solution with open APIs, gives multi-location or multi-entity healthcare organizations a shared chart of accounts, instant and continuous consolidations, amd centralized payables while eliminating manual processes for payments and intercompany accounting. Sage Intacct helps you save time and improve accuracy—without adding staff.



sage Intacct

Sage Intacct
300 Park Avenue, Suite 1400
San Jose, CA 95110

877-437-7765
sageintacct.com