Managing Third-Party Security and Privacy Risk: A Framework for Success

A Phreesia-CynergisTek White Paper

Phreesia

CYNERGISTEK

HEALTHCARE ORGANIZATIONS TODAY face greater challenges to privacy and security than ever before, as evidenced by the skyrocketing number of data breaches and cybersecurity incidents, such as ransomware attacks. In 2015, referred to by many as "The Year of the Healthcare Data Breach," the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) recorded a staggering 253 breaches, each affecting 500 or more individuals, totaling more than 112 million records.[1]

Why is healthcare experiencing such a sharp increase in breaches and security incidents? According to security experts, the answer is simple: Healthcare data is incredibly valuable. Containing a trove of sensitive information, including patients' names, Social Security numbers, birth dates and diagnosis codes, medical records fetch roughly $60 each on the Dark Web (i.e., websites that conceal their identity and location), compared with just $15 for Social Security numbers alone.

That price tag spikes to as much as $200 each for records that include both protected health information (PHI) and credit card data.[2] The cost to healthcare organizations that experience a data breach is enormous, averaging $363 per lost or stolen record, including fines, fees and remediation.[3] In addition to its financial impacts, a breach can have legal ramifications and lead to a tarnished reputation and a loss of patients' trust.

In this escalating threat landscape, it's not surprising that healthcare organizations are investing heavily in privacy and security through tighter security controls, enhanced monitoring and other preventive measures. Eight-five percent of healthcare organizations that responded to PwC's 2015 Global State of Information Security Survey had experienced a breach in the previous 12 months, and 63% said they planned to spend more than $1 million on security in the coming year.[4]

But even if provider organizations diligently adhere to best practices, they have another vulnerability to consider that's far more difficult to control: the privacy and security practices of their third-party partners. As healthcare organizations increasingly rely on outside vendors for a wide range of services involving PHI, they must ensure that those partners have robust policies and procedures in place to meet the highest privacy and security standards.

As healthcare organizations know too well, however, accurately assessing third-party vendors' privacy and security practices is no easy task. Despite companies' ubiquitous claims that they are "HIPAA-compliant," in truth, there is no rubber stamp or reliable shorthand that guarantees that an organization complies with HIPAA standards.

That uncertainty is a sore spot. In a recent Ponemon Institute survey asking companies about security risks among their third-party partners, nearly half of respondents said their organization had experienced a breach caused by one of its vendors, but only 31% said they had an effective vendor risk-management strategy in place.[5]

Ultimately, before healthcare organizations can entrust sensitive patient data to third-party partners, they must proactively and vigilantly assess their partners' controls and compliance with ever-changing privacy and security regulations. The onus is on healthcare organizations to perform appropriate due diligence to manage vendor risk, and identify partners that take privacy and security seriously.

About This White Paper

Phreesia and CynergisTek have co-authored this white paper to provide a framework of best practices that healthcare organizations can use to evaluate their third-party partners' privacy and security controls and risk-management practices to ensure they are compliant with HIPAA rules.

Because business relationships vary widely and regulations are constantly evolving, this framework—which is based on CynergisTek's review standards—is not intended to be a definitive checklist. Rather, Phreesia and CynergisTek have created this list of best practices to guide and simplify vendor risk management and provide clarity about the most critical areas for devoting resources and close attention. With this framework and vendor-review questionnaire (Appendix), healthcare organizations will be able to distinguish third-party partners that have built a strong culture of privacy and security compliance from those that are merely checking a list of boxes.

Assessing Security

Third-party vendors vary widely in how vigilantly they safeguard electronic protected health information (ePHI) from unauthorized access and use. While each healthcare organization will have its own top-priority criteria to be used when conducting vendor security reviews, the following list of best practices can help determine vendors' security processes and their willingness to comply with a healthcare organization's expectations.

An effective third-party vendor that values security should:

1.

CONDUCT REGULAR SECURITY RISK ASSESSMENTS

Verifying that a vendor has conducted an information security risk assessment should be an imperative when healthcare organizations review a vendor's security program. Risk assessments should be conducted on a regular, ongoing basis and reviewed and updated in response to changes in technology and the operating environment.

At a minimum, security risk assessments should: 1) evaluate the likelihood and potential impact of risks to ePHI, 2) institute measures to protect against those risks, and 3) document the security measures taken.

Vendors must also regularly review the findings of risk assessments to determine the likelihood and impact of identified risks, as well as determine how to remediate any deficiencies. Both CynergisTek and the OCR recommend using NIST's information security risk management framework (SP 800- 30) and the cybersecurity framework, which provide standardized methodologies for managing security and assessing risk.

In addition to performing internal risk assessments, many vendors turn to an outside firm that specializes in healthcare privacy and security, such as CynergisTek, to conduct a comprehensive risk assessment and recommend subsequent improvements. Enlisting outside help can provide valuable expertise, up-to-date information on the latest threats and a more rigorous review.

2.

HAVE A DESIGNATED SECURITY OFFICER

One good sign that a company takes security seriously is the presence of a knowledgeable senior-level executive tasked with developing and implementing information security efforts. Information security concerns can sometimes be at odds with other business objectives—speed, ease of operations, profit—and designating a senior leader who understands risk and makes security a priority sets a tone for the organization that is essential to building a culture of compliance.

3.

APPLY INFORMATION SECURITY MANAGEMENT PROGRAM ACROSS ALL OF ITS IT SYSTEMS

Consistency is the hallmark of a well-run security program. Applying different rules to different IT systems, especially when the systems are located within the same network, creates scenarios in which it's easy for a stressed system administrator to make a simple mistake, such as applying incorrect security configurations on a machine. Human error is one of the main causes of system outages and security breaches, so look for vendors that apply security policies uniformly across their IT systems and have regular testing to verify their configurations and security settings.[6]

4.

HAVE WRITTEN INFORMATION SECURITY POLICIES AND PROCEDURES IN PLACE

Written security policies and procedures should clearly outline the steps and tasks needed to ensure compliance and deliver expected outcomes. Without a written reference point, policies and procedures can become open to individual interpretation, leading to misalignment and mistakes. Healthcare organizations should confirm that vendors have comprehensive written security policies and procedures, and review them to ensure they align with their own standards.

5.

ENFORCE ROLE-BASED ACCESS FOR INFORMATION SYSTEMS THAT CONTAIN ePHI

Role-based access gives users access only to the level of ePHI they need to perform their job. Role-based access control within information systems bases the level of access to data on the position each user holds within an organization. For instance, a chief financial officer in most organizations would have little to no access to ePHI in his or her day-to-day role, while a database support technician might need limited access to troubleshoot an issue. Healthcare organizations should also ask their vendors if they enforce two-factor authentication for high-risk areas/users.

6.

HAVE PHYSICAL ACCESS CONTROLS IN PLACE TO LIMIT ACCESS TO ePHI SYSTEMS AND FACILITIES HOUSING ePHI

It's very easy to overlook the physical aspects of safeguarding ePHI, but loss and theft are among the leading causes of breaches. When evaluating a business partner's security policies and procedures, check to see that the company takes physical access seriously. Such good practices include requiring badges and escorts for visitors to data centers, using adequate employee validation practices (e.g., background checks) and keeping detailed logs of who accesses facilities to perform repairs.

7.

HAVE PROCESSES OR TOOLS IN PLACE TO INVENTORY AND MONITOR ALL DEVICES AND MEDIA THROUGH WHICH ePHI MAY BE ACCESSED OR MAINTAINED

Find out whether vendors have a comprehensive inventory of all of the hardware, software, laptops, tablets, mobile hard drives and other media that collect or store ePHI. An inventory is a necessity for effective information security because it's impossible for an organization to secure what it doesn't know it has.

8.

HAVE A DISASTER RECOVERY PROGRAM

In order to be compliant with the HIPAA Security Rule, vendors must have a detailed disaster recovery program that includes analysis on how a natural disaster—fire, flood, or even a rodent chewing through cables—could affect systems containing ePHI. The plan should also include policies and procedures for operating after a disaster, delineating employees' roles and responsibilities. Finally, the plan should clearly state a plan for restoring ePHI.

9.

ENCRYPT DATA IN TRANSIT, INCLUDING DATA STORED ON LAPTOPS, EXTERNAL HARD DRIVES, THUMB DRIVES AND APPLICATION DATABASES

Encryption, a process that protects data by making it unreadable without the use of a key or password, is one of the easiest methods of protecting data against theft. When a vendor tells you their data is encrypted, don't stop there. Delve deeper and ask for details about different in-transit scenarios, such as encryption of backup tapes. It's also imperative that the keys used to encrypt the data are very well-protected. Understanding how encryption keys are protected is as vital as encryption itself.

10.

HAVE ITS OWN VENDOR SECURITY MANAGEMENT PROCESS

A robust vendor security management process should include an inventory of vendors, an inventory of the data being shared with those vendors, and a program for reviewing vendors' security practices, policies and procedures (this paper should serve as a guidepost for that process). These criteria are in addition to meeting the HIPAA Security Rule requirements to have executed business associate agreements (BAAs) with any contractor or vendor that handles PHI on their behalf.

If a vendor has its own rigorous vendor security management process in place, it's a good sign that the company takes security seriously. As healthcare becomes increasingly interconnected and data flows among a wider variety of organizations, it's critically important that healthcare organizations ask vendors how they assess and manage risk with their own vendors.

11.

HAVE A 24X365 SECURITY OPERATIONS CENTER THAT MONITORS ALL SYSTEMS FOR POTENTIAL SECURITY ISSUES

Cyber criminals don't stop trying to hack into systems after normal business hours. Cybercrime is a global industry, and threats exist around the clock. Constant monitoring means a vendor can identify threats as they occur. The speed with which an organization spots an attack can mean the difference between an availability issue and a full data breach. A monitoring program process may be established internally and conducted by the vendor itself or implemented by another vendor.

12.

HAVE A PROCESS IN PLACE FOR IDENTIFYING AND RESPONDING TO INFORMATION SECURITY INCIDENTS

Security incidents run the gamut from the mundane to the severe, ranging from an email containing ePHI sent to the wrong address to a full-scale cyberattack on an information system. Identifying and drilling response protocols for both frequent and rare events helps ensure that an organization is adequately prepared.

Vendors that have a culture of compliance regularly conduct tabletop exercises using simulated events to test their processes. During a real security incident, tensions run high, and unless processes are well-drilled and staff are trained, it's easy for missteps to occur.

13.

HAVE A PROCESS IN PLACE FOR CONDUCTING BACKGROUND CHECKS AND SCREENING NEW HIRES

Having a consistent process for checking and screening new hires ensures, at the very least, that a company is validating that its employees are who they say they are and have the qualifications required to do their jobs. Vendors will vary in the frameworks they use to determine employees' risks to security, so healthcare organizations should ask for detailed criteria to be sure they align with their own screening processes.

Also, make sure vendors' screening processes include increased rigor for employees in positions of greater trust, such as system and network administrators.

14.

BE ABLE TO PROVIDE DOCUMENTATION

As part of vendor risk management, ask for relevant documentation, including copies of policies and procedures, trainings, background investigations, third-party security evaluations and facility assessments. While some companies may refuse to share actual copies of such documentation, they should be willing to review them in online meetings.

Culture of Compliance

Organizations that have instilled a culture of compliance view privacy and security not as a burdensome list of boxes to be checked during a once-a-year review, but as a set of systemwide priorities that affect every company decision. A culture of compliance starts at the top, with a committed senior leadership team that leads by example, and extends all the way to junior staff, with responsibility and consequences at every level. The goal is to ensure that each employee at every tier of the organization understands both the importance of safeguarding ePHI and how he or she helps fulfill that obligation.

Protecting Privacy

Healthcare organizations need to be confident that their potential third-party partners have the systems and safeguards in place to keep ePHI confidential. The following list of best practices can be used as a tool to evaluate vendor privacy policies and HIPAA compliance.

An effective third-party vendor that prioritizes privacy should:

1.

HAVE A DESIGNATED PRIVACY OFFICER WHO IS RESPONSIBLE FOR THE COMPANY'S PRIVACY PROGRAM

Vendors that handle sensitive information, including ePHI, should have a senior-level privacy official dedicated to ensuring that the vendor's business operations and employees comply with privacy regulations, policies and procedures. Larger vendors may have more than one person supervising these practices throughout the organization.

The privacy official's duties should include: developing, updating and administering privacy policies and procedures; monitoring business operations to ensure consistency with HIPAA requirements; working with product development teams to ensure that all products comply with applicable privacy standards; conducting mandatory employee training; and ensuring that business associate agreements are in place with contractors and vendors.

2.

HAVE WRITTEN INFORMATION POLICIES AND PROCEDURES IN PLACE TO ADDRESS HIPAA PRIVACY AND BREACH NOTIFICATION RULES

The HIPAA Privacy Rule encompasses an array of requirements, including the duty to account for disclosures of ePHI, the requirement to enter into a business associate agreement with a downstream business associate of the vendor, and the obligation to provide the patient with access to a copy of ePHI to the covered entity, the patient, or the patient's designee.

The HIPAA Breach Notification Rule requires vendors to provide notification to the covered entity following a breach of unsecured ePHI. The notification must contain, to the extent possible, the names of each individual affected by the breach and any other available information that the covered entity must provide in its notification to affected individuals.

Without written policies in place, it's impossible to make sure vendors are abiding by consistent standards.

3.

HAVE A PROCESS FOR MANAGING INCIDENTS INVOLVING UNAUTHORIZED USE OR DISCLOSURE OF ePHI

If a privacy event occurs—specifically an incident involving the unauthorized use or disclosure of ePHI—the vendor should, at a minimum, have policies and procedures for investigating, mitigating and documenting the incident.

4.

HAVE A PROCESS FOR APPLYING MINIMUM NECESSARY PRINCIPLES

When using or disclosing ePHI, or when requesting ePHI from a covered entity or another business partner, a vendor's employees must limit any use or disclosure to the minimum extent necessary to accomplish the intended purpose of the use, disclosure or request. For instance, if a vendor requires only a patient's medical record number to troubleshoot an issue with that record, then the vendor should only access the patient's medical record number. Accessing the patient's name, Social Security number, or clinical information in that instance runs afoul of the minimum necessary requirement. When a vendor maintains a culture of compliance, its employees are constantly asking themselves if the tasks they perform—no matter how routine or unique—adhere to these principles.

5.

HAVE A PROCESS IN PLACE FOR SUPPORTING A COVERED ENTITY'S DUTY TO AMEND ePHI WHEN IT HAS APPROVED PATIENT AMENDMENT REQUESTS

From time to time, patients may request to amend something in their medical records, such as information that was entered incorrectly by a physician or additional details they forgot during an initial visit.

HIPAA grants patients the right to request that a covered entity amend their ePHI or record maintained in their designated record sets. The covered entity may require patients to request such amendments in writing and provide a reason to support a requested amendment, provided that it informs patients in advance of such requirements.

If a vendor retains ePHI on behalf of a healthcare organization, then the vendor should have policies and procedures in place to honor requests to amend the patient's ePHI or medical record.

6.

HAVE TRAINING POLICIES FOR NEW HIRES AND EXISTING EMPLOYEES

As part of healthcare organizations' vendor-review process, they should check to make sure that a vendor's employees receive training on privacy policies and procedures when first hired. Vendors should also, at a minimum, conduct annual training to ensure that privacy and security policies stay fresh in their employees' minds. And because human error is one of the greatest sources of privacy and security incidents, vendors ideally should provide training on how to avoid malware attacks, including social engineering, such as phishing.

Cybercriminals use social engineering to manipulate or deceive users into

relinquishing control of their computer system and/or divulging sensitive information. Notably, a majority of cyberattacks begin with a "spear phishing" email. The email appears to be from a legitimate, familiar sender who attempts to elicit a specific response from the recipient. For example, the sender may ask the recipient to provide confidential information or to click on a link in the email. Untrained employees compromise an organization's security. Therefore, it is vital that employees receive training on how to detect and eliminate social engineering attempts.

In addition, annual training should be updated to reflect new regulations, industry standards and changes to business processes.

What is the Difference Between Security and Privacy?

Security

Put simply, security refers to the controls and processes that protect data from being accidentally or intentionally accessed by unauthorized individuals.

Privacy

Privacy, on the other hand, refers to the policies and procedures that control how patient data can be accessed, used and disclosed.

Extra Steps

Nothing can substitute for comprehensive risk assessments and adherence to HIPAA standards, as described in the framework above. However, there are some alternative approaches that can help further compliance goals that deserve attention.

HHS does not offer a product- or vendor-certification program, which makes it difficult to clearly demonstrate compliance and easier for some vendors to create the appearance of achieving it. Adhering to HIPAA standards and demonstrating that adherence requires commitment, discipline and rigor. Information privacy and security is not a bolt-on service or a package that can be purchased. Rather, as a best practice, it should be integrated into every process and procedure. Many vendors turn to outsourcers or consultants that offer HIPAA privacy and security "out-of-the-box solutions" or "stamps of approval" (e.g., "HIPAA-compliant"). While some aspects of such solutions may be valuable, take the time to really understand how the vendor operates its privacy and security programs. Go beyond a company's marketing materials and use the framework above to gain confidence that your data will be handled appropriately.

Beyond this framework, an organization can also demonstrate compliance by achieving certifications or attestations of compliance against security standards, such as the International Organization for Standardization (ISO), Payment Card Industry Data Security Standard (PCI DSS), Service Organization Controls (SOC), and the Health Information Trust Alliance (HITRUST). In order to achieve one or more of these certifications or attestations, a knowledgeable and trusted third party must conduct an audit and verify that the vendor is able to demonstrate compliance with the standard in question. Certification to the above standards can provide assurance, but it does not always tell the entire story, nor does it equal compliance.

Healthcare organizations might also find that some vendors tout the security certifications of the third-party partners that host their solutions. Be aware that those third-party vendors' certifications only cover a small subset of the overall control framework that applies to the vendor. Healthcare organizations need to verify that vendors address those privacy and security gaps, and they can use the above framework as a guideline for such validation.

Finally, vendors should be aware of state laws and regulations governing privacy and security, while also considering whether or not state requirements are preempted by HIPAA. For example, in the event of a security breach affecting individuals in different states, the vendor should evaluate the security breach notification laws in each affected state, in addition to HIPAA requirements.

Conclusion

The privacy and security framework detailed in this white paper is meant to be used as a guidepost in conducting the thorny process of vendor privacy and security review. While all the measures in this framework are essential for a robust privacy and security program, above all else, healthcare organizations should seek to partner with vendors that foster an organization-wide culture of compliance. Look for companies that can demonstrate they have made privacy and security top priorities, dedicated the necessary time, money, staff and resources to the effort, and whose commitment is reflected in all of the decisions they make.

A rigorous vendor assessment takes time, but the payoff—confidence that a partner's compliance program is rigorous and closely aligned with your own—is worth it.

About Phreesia

Phreesia's software gives healthcare organizations a suite of applications to manage the patient intake process. Their innovative platform engages patients in their care and provides a modern, consistent experience, while enabling clients to maximize profitability, optimize their staffing and enhance clinical care. Phreesia prioritizes privacy and security at every level of its organization and has been recognized with HITRUST CSF Certification, demonstrating adherence to industry-recognized standards and regulations. To find out how Phreesia can give your organization the capacity for more, visit www.phreesia.com.

About CynergisTek

CynergisTek is a top-ranked information security and privacy consulting firm. The company offers solutions to help organizations measure privacy and security programs against regulatory requirements and assists in developing risk management best practices. Since 2004 the company has served as a partner to hundreds in the healthcare industry. CynergisTek is also dedicated to supporting and educating the industry by contributing to relevant associations such as HIMSS, AHIMA, HFMA, HCCA, AHIA, AHLA, IAPP and CHIME. CynergisTek has been named in multiple industry research reports as one of the top firms provider organizations turn to for privacy and security.

Glossary

BUSINESS ASSOCIATE - According to HIPAA, a business associate is a person or entity that creates, receives, maintains or transmits protected health information on behalf of a covered entity or another business associate

COVERED ENTITY - HIPAA defines a covered entity as a health plan, healthcare clearinghouse or healthcare provider that electronically transmits health information in connection with transactions for which HHS has adopted standards

ENCRYPTION - A process of converting sensitive data into a format that is unreadable without a key or password

ePHI - Electronic protected health information that is covered under HIPAA Rules

HHS - The U.S. Department of Health and Human Services

HIPAA - The Health Insurance Portability and Accountability Act under which HHS promulgated standards for protecting the privacy and security of PHI

NIST - The National Institute of Standards and Technology, an agency of the U.S. Department of Commerce dedicated to advancing standards, measurement and technology

OCR - The Office for Civil Rights, an agency within HHS tasked with developing and enforcing the standards for health information privacy and electronic security standards for the protection of protected health information

RANSOMWARE - A type of malware that restricts access to a computer system in some way and demands a ransom payment to restore access to it

1. The U.S. Dept. of Health and Human Services Office of Civil Rights Breach Portal (Note: Figures include breaches affecting 500 or more records) https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

2. *Payment Card Data and Protected Health Information Security Practices* https://usa.visa.com/dam/VCOM/download/merchants/webinar-healthcare-data.pdf

3, 6. Ponemon Institute 2015 *Cost of Data Breach Study: Global Analysis* http://www-03.ibm.com/security/data-breach/

4. PwC *Medical Cost Trend: Behind the Numbers 2016* http://pwchealth.com/cgi-local/hregister.cgi/reg/pwc-hri-medical-cost-trend-2016.pdf

5. Ponemon Institute's *Data Risk in the Third Party Ecosystem* http://www.buckleysandler.com/uploads/1082/doc/Data_Risk_in_the_Third_Party_Ecosystem_BuckleySandler_LLP_and_Treliant_R....pdf

Appendix: Question List for Vendor Review

Phreesia and CynergisTek created this question list to guide your vendor-risk management efforts. Each question corresponds with a numbered best practice in the attached white paper. This list is not intended to be used in isolation as a definitive checklist, but rather as a tool that, along with the white paper, helps you assess how your vendor conducts their privacy and security activities.

SECURITY QUESTIONS		YES	NO
1.	Do you conduct regular security risk assessments?		
2.	Do you have a designated security officer?		
3.	Do you apply your information security management program across all of your systems?		
4.	Do you have written information security policies and procedures in place?		
5.	Do you enforce role-based access for information systems that contain ePHI?		
6.	Do you have physical controls in place to limit access to ePHI systems and facilities housing ePHI?		
7.	Do you have processes or tools in place to inventory and monitor all devices and media through which ePHI may be accessed or maintained?		
8.	Do you have a disaster recovery program?		
9.	Do you encrypt data in transit, including data stored on laptops, external hard drives, thumb drives and application databases?		
10.	Do you have your own vendor security management process? Can you provide documented BAAs?		
11.	Do you have a 24x365 security operations center monitoring all systems for potential security issues?		
12.	Do you have a process for identifying and responding to information security incidents?		
13.	Do you have a process for conducting background checks and screening new hires?		
14.	Can you provide documentation, including copies of policies and procedures, trainings, background investigations, third-party security evaluations and facility assessments?		

PRIVACY QUESTIONS		YES	NO
1.	Do you have a designated senior-level individual who is responsible for your company's HIPAA privacy program?		
2.	Do you have written information privacy policies and procedures in place to address the HIPAA Breach Notification and Privacy Rules?		
3.	Do you have a process for managing privacy incidents?		
4.	Do you have a process for applying minimum necessary principles for use or disclosure of ePHI?		
5.	Do you have a process in place for supporting a covered entity's duty to amend ePHI when it has approved a patient amendment request?		
6.	Do you have training policies for new hires and existing employees?		