Beyond Compliance: Strategic Risk Management at HIA in a Shifting Threat Landscape

As the new CISO of HIA, it is my job to understand the constant changes within the cyber threat landscape, especially in the highly targeted and regulated industry that is healthcare insurance. My ability to stay ahead of the ever-evolving threats directly impacts the confidentiality, integrity, and availability of sensitive patient information and organizational data. It is also my responsibility to be able to educate our employees and other leadership on the importance of security, and why it matters.

First off, it is important to note that the cyberthreat landscape encompasses all potential and known cybersecurity risks that could harm users, organizations, industries, or time periods – and there are many reasons why it is evolving/changing so rapidly. (Chipeta, 2022)

The threat landscape changes every time a new event causes a significant shift or impact, and threats also evolve faster than any static security measures. There are many different types of cyber threats that become more sophisticated on a daily basis. Some of the common cyber threats include malware, social engineering attacks, ransomware attacks, zero-day vulnerabilities, and human error. Cybercriminals are continuously adapting their tactics, techniques, and procedures (TTPs) – we should be doing the same thing. What was secure a short time ago may very well now be vulnerable due to new malware strains, phishing techniques, or exploitation of previously unknown zero-day vulnerabilities. Leaving a security program to go stale, means risking leaving critical systems exposed. We work in a high-value target industry – healthcare. We handle vast amounts of PII and PHI, which makes us a prime target for any sort of threat/attack. If we can stay on top and understand the emerging threats, we can proactively defend against them, rather than reacting after the damage is done. This could easily destroy our reputation, our customers would have very little to no trust in us, and we would risk our customers' information leaking to anybody and everybody. It is not worth our being ahead of the game. Following on this, as we are in the healthcare industry, there are regulatory and legal pressures that we have to adhere to. We must stay in compliance with laws such as HIPAA, HITECH, and state data privacy regulations. This depends on us implementing "reasonable and appropriate" safeguards. By staying current, it ensures that our risk posture aligns with both legal expectations and industry best practices. We want to strive to be a company that others look to in respect to our security, and by understanding how threats are changing, we can adjust our program budgets, security priorities, staffing, etc., accordingly. We can take these newly allocated items and invest in areas with the highest risk exposure, rather than overfunding in the areas that are less vulnerable. With staffing, our team is not green – many of them have been here 5+ years. This could be challenging for some, but with leadership support/backing, and good management/leadership style, I want to empower and update the existing staff, as they are still operating under the prior CISO's security program and outdated assumptions at this point. If I understand the latest and emerging threat vectors, then I can reskill/skill-up the staff, aligning their practices with the current realities/future forethought, and improve their ability to respond more effectively. We all have to have a deep understanding of these current threats – it will enable us to have a more realistic and effective incident response plan(s). It ensures HIA is not only prepared to defend against attacks, but also to recover quickly, minimizing disruption to healthcare services and member trust. We want to remain available. In short, a dynamic approach to the cyber threat landscape for us is not optional – it is foundational. As the CISO, I am required to continuously assess the emerging risks to build a security strategy that protects patient data, meets compliance standards, and strengthens our organization's resilience against current and future attacks.

As the new CISO of HIA, protection of our customers' electronic ePHI is of the utmost importance. There are a variety of ways to identify information assets, but I would take a structured approach in order to pinpoint what holds value and needs protection. It is a critical first step in building an effective risk-based security strategy.

1. Comprehensive Data Inventory and Mapping:
   I would start out the process by having the team perform a system-wide audit. This would need to be done to locate, catalog, and classify all of our data assets. We need to understand where our data is stored – if it is on premises, in the cloud, endpoints, etc. – how it flows across our systems, and who can and is accessing it. As the new CISO of the company, I don't know everything that exists, and without that knowledge, I cannot protect it. We need to keep a data inventory. This would reveal any unknown or forgotten IT systems, undocumented data repositories, legacy applications that could still hold sensitive information, etc. In order to do this, we would use data discovery tools – such as Spirion or Microsoft Purview - to find unsecured ePHI, understand the data flows, and enforce HIPAA compliance by providing data visibility and control. We would implement data loss prevention (DLP) solutions – possibly Microsoft Purview or Google Cloud DLP - to monitor and control our data movement, it would help to prevent the unauthorized sharing of our data, as well as classifying and protecting this sensitive information, and it would support our compliance and reporting initiatives. We would also put automated

asset mapping platforms in place as well. These provide a graphical representation of our network infrastructure, so we can quickly discover any network connections, troubleshoot problems, meet network regulations, and we can plan for our future growth. NetBrain is a potential option here.

2. Engaging in Cross-Departmental Asset Identification
   This initiative is all hands-on deck across the company – we don't want silos for security, but rather collaboration with our common goal of protecting our and our customers' data. We will be in collaboration with the various business units to identify the information assets that are critical to their operations. This will help to uncover business-critical data that may not necessarily visible from a technical perspective. Our business units, and BU's in general, within the healthcare industry especially, often manage and use sensitive data in various ways that IT may overlook. With us being directly involved, it shows our dedication to the initiative, builds alignment with our teams, increases accuracy, and creates shared accountability for our data protection. Also, we want this to be a full organization priority – this will help to promote that security-aware culture.

3. Review System Logs, Access Controls, and Configuration Management Databases (CMDBs)
   We need to analyze the logs from the security information and event management tools and the infrastructure monitoring tools that are currently in place. We need to do this in order to identify which systems are storing and/or processing sensitive data. CMDBs can provide a structured inventory of hardware and software assets that are tied to our data workflows. This is all important because we need insight into which systems are actually being used to access, process, and/or transmit ePHI – by doing this, we can identify critical endpoints and potential vulnerabilities. Again, just stepping into this role, I'm not fully aware of everything that was in place and occurring. This helps to offer a real-time and historic views of our asset usage, which can help us to prioritize our protection efforts.

   With these three approaches – technical discovery, stakeholder engagements, and system analysis – we can build a complete, accurate, and risk-aware asset inventory, which is foundational for us to prioritize protections, meeting HIPAA compliance, and to defend against costly breaches.

HIPAA establishes federal standards protecting sensitive health information from disclosure without a patient's consent. (CDC, 2024)

Healthcare providers, healthcare plans, healthcare clearinghouses, and business associates are all subject to the Privacy Rule and are covered entities. HIPAA outlines administrative, physical, and technical safeguards that covered entities and business associates must implement to ensure the confidentiality, integrity, and availability of ePHI. (U.S. Department of Health and Human Services, 2024)

- Administrative Safeguards:
  These are the policies and procedures that manage the selection, development, and enforcement of security measures. Some of the key requirements that reside under this category are the Security Management Process, which is conducting risk assessments and implementing risk mitigation strategies. Assigned Security Responsibility designates a security official (this could be me as the CISO) that is responsible for HIPAA compliance. Workforce Security ensures proper access for authorized users, and restricts it for others, and Security Awareness Training provides ongoing training for employees on data protection and threat awareness. An Incident Response Plan implements procedures to respond to and document security incidents and breaches.

- Physical Safeguards:
  These safeguards protect the physical environment where PHI is accessed, stored, or transmitted. Facility Access Controls restrict physical access to data centers and workspaces to only authorized personnel. Workstation Security ensures that devices that are used to access ePHI are secure and used appropriately. Device and Media Controls include policies for the disposal, reuse, and movement of hardware or electronic media – for example, secure disposal of hard drives containing PHI, and even printers.

- Technical Safeguards:
  Technical safeguards are the technology and related policies that are used to protect ePHI and control access. Access Controls implement unique user IDs, role-based access, and login requirements to control who can view and/or alter ePHI. Audit Controls are those that track access and activity through logs and monitoring systems. These, again, are often handled by a SIEM tool. Integrity Controls protect data from improper alteration or destruction – which include things such as checksums and hashing. Authentication verifies that people and/or systems accessing ePHI are

actually who they claim to be. Transmission Security encrypts data during transmission (ie. Using TLS) to protect against any interception or tampering.

- Other Key Requirements:
  Some additional key requirements are Data Encryption – which is actually recommended, not explicitly required, but it is considered an "addressable" safeguard, which means that if it's reasonable and appropriate, then it should be implemented. Business Associate Agreements, or BAAs, are required for third-party vendors that access PHI, ensuring that they are also compliant. Last, the Breach Notification Rule, which requires covered entities to notify any affected individuals, HHS, and sometimes even the media if a breach of unsecured PHI occurs.

Overall, Administrative safeguards focus on policy and oversight, and cover things like risk analysis, training, and incident response. Physical safeguards focus on physical access and environment, covering locked server rooms and secure disposal of equipment/material. Technical safeguards focus on systems and data protection, covering encryption, access controls, and audit logs. Under HIPAA, organizations handling PHI are required to implement a comprehensive set of these safeguards to ensure the confidentiality, integrity, and availability of PHI. Together, these measures create a robust framework for protecting sensitive health information and maintaining compliance with federal law.

Policy framework matters. A well-defined Information Security Policy Framework is vital for ensuring that HIA can effectively identify, protect, and manage its most critical information assets, including ePHI, claims, patient data/communications, financial records, and employee information. Being the new CISO – reviewing the framework allows my team and I to (re)establish clear guidance and accountability around how these sensitive assets are handled, accessed, and protected across the organization. So why does this all matter at HIA?

1. Aligns Security Practices with Regulatory Obligations, such as HIPAA:
   We must comply with the strict legal requirements for protecting ePHI. Having a comprehensive policy framework ensures that the administrative, technical, and physical safeguards are mapped to HIPAA mandates. For example, our policies on access control and data retention must align with HIPAA's minimum necessary use and recordkeeping standards.

2. Standardizes Asset Classification and Risk Prioritization:
   Without consistent standards and procedures, our teams may interpret risk/asset value differently. A framework provides a more uniform classification system that ranks assets by sensitivity and impact. Patient health records and claims data should be classified as “critical” because of their high confidentiality, whereas anonymized analytics data would be “low”.
3. Enables Consistent Risk Assessment and Decision Making:
   By reviewing the current policies, we can ensure that the data discovery, risk assessments, and incident response procedures are all properly aligned with the value and risk level of each asset. If we discover something that is outdated or has conflicting standards, we may be overprotecting a low-risk system or even under-protecting the high-value ones.
4. Drives Accountability and Security Culture:
   When we clearly define roles, responsibilities, and procedures, we are ensuring that the departments that are handling sensitive data understand their obligations. With more and more use of mobile devices, standards ensure that staff accessing PHI on tablets, etc. are doing so in a secure manner, therefore minimizing risk from BYOD or remote work.
5. Supports Continuous Improvement:
   A strong policy framework includes feedback and periodic reviews. We will not let this go stagnant in a volatile environment. As we reassess information assets and uncover new threats, the framework ensures that our security controls are updated and enforceable.

The security policy framework is not just a documentation requirement. It is the foundation of how HIA classifies assets, mitigates risks, and ensures regulatory compliance. By consistently reviewing and strengthening it, we are creating a shared, enforceable structure that helps protect our most sensitive data, and supports both operational effectiveness and legal accountability.

As the CISO, my role includes assessing the current risks, reviewing and updating the security program, and adjusting budgets and resources accordingly. A risk assessment provides the baseline intelligence that I need to understand the ever-evolving threat landscape, especially what is specific to healthcare insurance, as it can help to identify where HIA’s most sensitive assets are exposed, and aid with making strategic, risk-based decisions about staffing, tools, policy updates, etc.

Risk assessments identify vulnerabilities and threats to our ePHI. We can pinpoint where sensitive data resides and identify the potential weaknesses, such as outdated software. Not all systems/threats carry equal weight, and a risk assessment can help us prioritize risks based on business impact. It evaluates the likelihood and impact of threats to determine which areas require immediate attention and resource allocation, and which don't at that moment. As the new CISO, I need to be able to make informed decisions. I am the one to reallocate budgets and re-assign staff to areas that are of higher risk. The assessment provides evidence to justify the decisions based on actual exposure, and not just assumptions. I want to truly ensure compliance with HIPAA and other regulations for HIA. HIPAA requires covered entities to conduct periodic risk assessments as part of the Security Management Process (§164.308(a)(1)), and a through, documented risk assessment helps to demonstrate compliance during audits and/or investigations. (Department of Health and Human Services, 2005) Risk assessment findings directly inform updates to security policies, controls, and procedures. If we have a weak multi-factor authentication method that is identified, the insight can help drive new access control policies.

Risk assessments are critical for aligning security efforts with actual threats. They help HIA protect sensitive health data, they ensure regulatory compliance, and they allocate limited resources to the areas of the greatest risk – which makes them central to the effectiveness of my role as CISO.

As the newly appointed CISO at HIA, my primary responsibility is to strengthen the organization's security posture by assessing current risks, reallocating resources, aligning security practices with regulatory requirements, etc. – especially those related to the protection of ePHI. It is critical that I understand the evolving cyber threat landscape, which then enables me to proactively defend against modern threats. Protecting our customers' data isn't just a technical challenge – it is a legal and ethical obligation that is governed by laws such as HIPAA, which mandate administrative, physical, and technical safeguards for PHI. In order for us to fulfill these requirements, we must identify and classify HIA's information assets utilizing a variety of tools, by conducting thorough risk assessments, and implementing a strong Information Security Policy Framework to ensure consistent, organization-wide adherence to best practices, compliance standards, and proper handling of sensitive data.

Ultimately, the effectiveness of me being the CISO depends on building a strategy that combines legal compliance, ethical responsibility, and technical defense, thus creating a secure, resilient environment that protects HIA's data, reputation, and patients' trust.

References

5 Best Network Mapping Tools. (2024, July 17). UVexplorer. https://www.uvexplorer.com/articles/top-5-best-network-mapping-software/

Barney, N. (2022, December). *What is telemetry and how does it work?* WhatIs.com. https://www.techtarget.com/whatis/definition/telemetry

CDC. (2024, September 10). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Public Health Law; Centers for Disease Control and Prevention. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

Chipeta, C. (2022, August 18). *What is the Cyber Threat Landscape? | UpGuard*. Www.upguard.com. https://www.upguard.com/blog/cyber-threat-landscape

Department of Health and Human Services. (2005). *What is the Security Series?* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

Fink, L. (2019, August). *Healthcare Data – Hold on to Your Assets!* Haugen Consulting Group | Healthcare Consulting, Education, and Auditing. https://www.thehaugengroup.com/healthcare-data-hold-on-to-your-assets/

How to choose data discovery tools: 8 features. (2024). Ataccama.com. https://www.ataccama.com/blog/data-discovery-tools

Kappel, R. (2025, January 9). *Top 10 Data Loss Prevention (DLP) Tools for 2025*. Centraleyes. https://www.centraleyes.com/top-data-loss-prevention-tools/

U.S. Department of Health and Human Services. (2024, December 30). *Summary of the HIPAA security rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

What is the Cyber Threat Landscape? | UpGuard. (2022). Upguard.com. https://www.upguard.com/blog/cyber-threat-landscape#toc-1

What is the Threat Landscape? (2025, January 16). SecurityScorecard. https://securityscorecard.com/blog/what-is-the-threat-landscape/