Securing and Operating Healthcare Data Environments

July 2022

Table of Contents

White Paper Purpose

Healthcare data and the organizations that house and use this data are at the forefront of cyber-attacks across the globe. This White Paper discusses the challenges involved in operating computing environments that house and utilize sensitive protected healthcare data in the United States. It discusses cybersecurity threats, practices that need examination, and standards, certifications, and compliance. This paper also provides a practical set of actions to help organizations establish and improve their operational and security posture and concludes with our recommendations on improving security posture.

The threat landscape for healthcare data is ever growing. Today consumers, researchers, providers, and payers access and exchange information electronically as part of the emerging interconnected healthcare system. However, healthcare data, relative to financial, credit, and eCommerce-based retail industries, is a late comer to internet accessible sites and electronic information exchange. Users expect system interactions to be as frictionless as possible; the security implications of this shift to electronic data reliance for the healthcare industry are significant. Every player in the data interchange ecosystem that experiences a breach affects all of its direct and indirect partners***. On a weekly basis there is at least one news report detailing a healthcare entity suffering a risk to their data security including data breaches***.

Risk is inherent in every business activity, and security risks in the healthcare field of utmost importance to every organization operating in this space. Businesses that house and use the most sensitive data about a person, Protected Health Information (PHI) and Personal Identifying Information (PII) have a critical responsibility as the stewards of that data to ensure they protect the rights and privacy of the individuals.

This paper is especially important for organizations whose business touches PHI and PII yet may lack the resources or experience to be good stewards of PHI and PII. Understanding the laws, regulations and certifications, security skills, tools, and practices may not have been the initial investment focus of a nascent research or IT development organization in the healthcare domain; a path to securing their business can be longer and more expensive than anticipated. This paper provides guidance to help manage healthcare data-related security risks and helps ensure businesses can securely focus their core activities in a cost effective and value-focused manner.

Threats

Breaches: It is no surprise to healthcare and IT security industry participants that healthcare data has become a prime focus for malicious intent actors. According to Becker's Hospital Review[1] almost 50 million Americans had their sensitive data taken from one of the entities that was holding or using that data for legitimate business reasons. Some of those entities are providers, including hospitals, clinics and physician practices, payer

[1] https://www.beckershospitalreview.com/cybersecurity/healthcare-data-breaches-by-the-numbers-9-stats.html

organizations, and support organizations. For example, an eye care software vendor placed some of Texas Tech University's data at risk in 2021[2].

With these healthcare breaches increasing at almost 20 percent per year, healthcare organizations should be prepared for the threat to continue well into the future. Actions ranging from data theft to ransomware cost the healthcare industry over $9.2 million on average for every breach according to a report from IBM[3]. Even if an organization does not think the data that it holds is PHI/PII, the possibility exists that they have sensitive data – "caution" is the watchword[4].

Threat Vectors: The ability for hackers to gain access to sensitive data is growing, aided by many factors, including open-source tools that target vulnerabilities in software, a high volume of new complex code bases to operate healthcare infrastructure, and sophisticated attack campaigns on the human entry points to IT systems. Significant attention must be focused on the human vulnerability points such as email phishing campaigns, insider malicious actors, and other than email-initiated malware entry.

This paper is focused on establishing environment and control processes to present a hardened surface for the IT environments to reduce these risks, such as threats from unpatched servers, improperly bestowed access credentials, unencrypted data in various states, and other associated entry points.

Practices That Need Examination

This paper discusses several areas of system development and administration-specifically Integrated System Development, Agile, and the CI/CD pipeline. The sensitivity and regulation around healthcare data, and the risks inherent in being the steward of this data require rigor in all aspects of the IT processes and infrastructure.

Integrated System Development Approaches: The integration of development, security, and operations (DevSecOps) overlaps with environmental protections. How you develop software effectively requires cooperation across the IT and business enterprise. DevSecOps (also expressed as SecDevOps) is integrated IT models and is a critical part of end-to-end security strategies. We recommend that the impact of PHI and PII privacy laws and regulations and the security guidance for that specialized data become part of the organizations culture and integral to the program management picture.

Integrating commercial software capabilities are part of the sphere that will be influenced by higher level security needs. The organization must ensure the base commercial product meets strict security guidelines and certifications outlined in Section 5; however configurations, integration points, environments, and the testing and deployment pipeline are all malleable areas that the organization can affect, impacting the risk profile.

[2] Texas Tech Health Science Center's vendor breach affects 1.2 million patients (beckershospitalreview.com)

[3] https://www.ibm.com/downloads/cas/OJDVQGRY

[4] Bloomberg News reports) that Meta is facing a lawsuit regarding private medical data ending up on Facebook. https://www.bloomberg.com/news/articles/2022-06-17/meta-sued-over-claims-patient-data-secretly-sent-to-facebook

Agile – On a Tightrope: The advent of Agile IT development has improved the capabilities delivered to IT capabilities users and has sped up the overall process of delivering capabilities while reducing the risk of wasting money on features that are not usable or useful.

The Program Management Institute (PMI), one of the world's most influential program management organizations has adopted in critical Agile tenets to its widely accepted teaching and credentialing due to the value of Agile approaches[5]. Full treatment of these approaches can be found in PMI's materials, as well as other organizations like the Manifesto for Agile Software Development organization[6].

We recommend that stewards of healthcare data should examine and adjust Agile approaches and adjust them to help protect healthcare data. The "fail fast" principle must be balanced against absolute best efforts to protect privacy. Testing regimens and speed-to-market must be adapted whenever the organization holds healthcare data, including steps such as examination for OWASP top ten vulnerabilities[7] and added vulnerability and penetration testing, This testing is in addition to the performance and functional value testing integral to delivery. While many industries can afford the risk of bringing error in their product to market, a healthcare steward cannot use that model because of potential life threatening consequences. Agile needs to adapt to the risk level of the application, data, and its use.

CI/CD Pipelines: Integrating IT development with IT operations provides an acceleration factor to move from concept to functional reality supporting the business operation, customers, and in many cases, patients and families. Automation can further accelerate the process. Integration of security concepts to identify flawed code and development processes in the pipeline is critical when moving from DevOps to DevSecOps. If an organization does not yet infuse security architecture, design and development techniques in every stage of the pipeline we recommend that change as soon as possible. Many organizations espouse that approach, however an effective strategy requires changes in policy and automation levels as well.

Infrastructure standards covering services and a standard configuration base for IT capabilities implants consistency across the organization and its developers. We recommend implementing standards into systems infrastructure at all levels: development, test and production. Consistent images, use of the same services and commercial products and the same architectures, by every developer reduces risks whether the IT product is a product or developed software. Verifying compliance can most effectively be achieved by maximum automation of testing such as the inclusion of static and dynamic testing with required passing grade factors. Penetration testing is a critical tool to be part of standard processes but is usually outside an automated pipeline and often contracted, even in large organizations. Smaller organizations do not always have the expertise or the rigor to incorporate standards and automated testing, but in concert with staff training regarding human attack vectors

[5] https://www.pmi.org/learning/featured-topics/agile

[6] https://agilemanifesto.org/

[7] https://owasp.org/www-project-top-ten/

and comprehensive environment configuration and patching this approach provides critical protection layers for effective risk reduction.

Standards, Certifications, and Compliance

Achieving measurable compliance with required and effective security practices (using the associated 'badges' to identify these achievements) is critical for healthcare data stewards. Individual certifications, such as a Certified Information Systems Security Officer – CISSO and environmental certifications and audits (such as HITRUST), are a reflection of solid security practices, demonstrating reasonable efforts to protect individual privacy and to protect the organization's reputation. These actions are more than recommended; they are a must for organizational credibility, as well as reasonable risk reduction. Federal standards are an excellent guidepost that reduce risk. The U.S. federal government, at a regulatory level, is notoriously risk averse; combined with expertise housed across agencies (including the National Institute of Standards and Technology (NIST)), it produces guidance, practices, and legal requirements to provide adherence.

The following table provides common acronyms regarding security and privacy laws, regulations, standards, and certifications.

Acronym or Name	Description
CISA	**Cybersecurity and Infrastructure Security Agency** is the federal agency responsible for national cybersecurity concerns. Among other activities, it monitors cyber threats, maintains a National Cyber Awareness System, and issues alerts industry and the public on an ongoing basis.
CCPA	**California Consumer Privacy Act**. This law gives individuals more control over their privacy than other statutes do. Implementation of provisions is complex and federal-state preemption boundaries add some complexity.
FEDRAMP	**Federal Risk and Authorization Management Program**. FEDRAMP is a certification for commercial cloud products regarding security controls and authorizations for federal agencies use. Federal agencies must sponsor a product for their use for the commercial product to be so certified.
FIPS	**Federal Information Processing Standards** (FIPS) are standards and guidelines for federal computer systems that are developed by National Institute of Standards and Technology (NIST) in accordance with the FISMA.
FISMA	**Federal Information Security Management Act**. Legislation that sets the target for guidelines and standards for federal information security on IT systems. NIST's FIPS are structure to be the embodiment of how to be FISMA compliant. Systems can be rated as FISMA Low, Moderate, or High impact compliant; most federal health care data environments must be FISMA moderate compliant.
GDPR	**General Data Protection Regulation (GDPR)**. GDPR is a European Union (EU) law governing privacy and human rights. It is the equivalent of HIPAA for healthcare data purposes across the EU and its citizens. Notably the rights for the data belong to the individual wherever they are, and regardless of whomever is holding or using the data.

Acronym or Name	Description
HIPAA	**Health Insurance Portability and Accountability Act**. Among other main points this law establishes a baseline of requirements / standards for stewards of PHI to comply with privacy protections for individuals. The Act was passed in 1996 with multiple new laws adjusting it in the past 26 years.
HITRUST	Health Information Trust Alliance. HUTRUST is an alliance that authorizes contractors to assess IT environments and systems and issue compliance with HITRUST's requirements. A HITRUST certification of compliance is equivalent with meeting FISMA moderate requirements, and meets HIPAA security requirements, thus becoming a public demonstration for private healthcare data stewards to the market that they have effective security tools, controls and environments.
NIST	**National Institute of Standards and Technology**. NIST is a broad ranging federal agency that "advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life"[8]. NIST's security and privacy controls and practice publications (such as NISTP Special Publication 800-53) are the foundation used for most federal security requirements and the bedrock of FIPS standards and HITRUST certifications, among other uses.
OWASP	**Open Web Application Security Project.** This non-profit foundation supplies tools and resources to support secure IT capabilities, its 'Top 10' are a notable set of (ever changing) flaws for every development organization to take note of and insure they are not present.
Privacy Act	**The Privacy Act** sets governing rules and standards for PII that is held and used by federal agencies to protect the privacy of the citizenry.
SOC	**System and Organization Controls**. These controls are defined by the American Institute of Certified Public Accountants. A SOC-2 level of compliance demonstrates a level of control and oversight on IT environments. A SOC 2 level audit is a good basis for security practices but is not sufficient for PHI/PII rich environments, it is not as rigorous or accepted as a HITRUST certification or FISMA moderate compliance.

As stated above, healthcare data is a prime target for malicious actors, with many assessing healthcare data as having a higher value to those actors than credit information. HITRUST certification for environments and processing systems demonstrates that the organization is following the proper level of procedures, tools, and controls for customers, business partners, and external oversight organizations. () This level of public certification assures customers and downstream service consumers that their provider is taking the utmost level of care to reduce risk and protect their data. For organizations supporting federal agencies, FISMA moderate (and when appropriate, FEDRAMP) certifications will be required.

[8] NIST.gov

Planning Recommendations

Recommendations regarding methodologies and approaches to securing a healthcare entities IT environments and systems have been made in the preceding sections. The following information will help tie together the steps to achieve an ongoing culture and process for an organization to keep the risk levels properly managed regarding their sensitive mission.

Overall Thoughts: Securing a healthcare business and its electronic data is a comprehensive undertaking. HIPAA in the 1990's began to crack down on sloppy business practices (e.g., placing printed member ID cards containing PII and PHI in a dumpster prior to shredding) and IT security issues by enforcing fines and criminal liability as consequences of negligent actions. HIPAA-aligned security programs must address the integrity of the IT systems infrastructure, including access controls and monitoring procedures as well as technical elements supporting prevention, detection, and remediation of issues.

Planning Steps for Securing Infrastructure: At a high level when considering how to plan for securing infrastructure here are analytic and data gathering and planning steps we recommend:

1. Assess what data you will be holding and touching.
2. Assess what markets (businesses, individuals, locales, and jurisdictions) you will be in. Keep in mind that the jurisdiction and its rules may follow the person, such as a European national with data included in a U.S. jurisdiction. Know the rules, regulations, and laws that apply to your business
3. Assess the buyer market's risk profile-those consuming your products and services will look for their actual and perceived needs to be met.
4. Build your risk profile based on the data gathered.
5. Build IT plans including application development, operations, and security processes using an integrated DevSecOps approach.
6. Construct a target state based on the data gathered and the risk profile. Remediation such as excluding some data to change the jurisdictional profile may be part of the target state.
7. Create a plan and budget to get to the target state.

Industry Expectations: As stressed in the above sections, we highly recommend obtaining a HITRUST certification for the hosting and processing of PHI and PII sensitive data. Regarding security, certifications, and experience the healthcare industry has expectations for any products and services they consume. For IT applications and infrastructure, demonstrating the right control tools and capabilities, usually via certifications, are a key component of meeting those expectations. For instance, some private sector healthcare entities will look for a SOC-2 audit, but many will look for HITRUST certifications, and in a competition the HTRUST certification will be a winning strategy for the seller of services. In the government space, being FISMA moderate compliant is required to operate environments on behalf of the federal government, and products in use in that marketplace strive for a FedRAMP certification. Federal agency works for hire, however, will not be FedRAMP certified, thus FISMA compliance is their level of requirement. Note that FISMA high compliance is rarely required for healthcare data in the government and has an expensive cost impact to the agency when it is required.

Achieving Compliance: When a company's needs and risk profile are defined, actions should be taken to achieve the compliance needed to both properly safeguard the information and to demonstrate these safeguards via audits and certifications. Hundreds of controls, active monitoring (tools, staff, and functions such as a SOC), ongoing monitoring of trends (OWASP Top 10, CISA alerts, and vendor patches, etc.), and other activities are part of establishing and maintaining a secure, certified environment and application.

Large multi-billion dollar organizations will maintain a comprehensive security/cybersecurity operation and will have a significant investment in staff and other resources to secure their business and the data they maintain. Smaller organizations may need to initiate security programs if they have not begun to do so. A HITRUST certification will require significant time to achieve (often nine months or longer) with fees for outside certifying organizations (a requirement) and possibly outside security consultation expertise (often a necessity) that can be the high six figure dollar range or more. Alternatives for portions of the security program to consider include:

- For a software service provider (Software as a Service (SaaS)) where the infrastructure itself is not the unique product, consider hosting the processing in a vendor's environment with specific healthcare data expertise and that has already achieved HITRUST or FedRAMP certifications. A SOC-2 audited vendors operation will not provide enough market assurance
- For an infrastructure solution vendor, consider using certified products to surround your offering, build the minimum you need to build to reduce your overall audit and certification effort.

The landscape changes daily, and requirements change frequently, as a result. For instance the federal government is moving rapidly toward all access being controlled in a 'Zero Trust Architecture,' which includes concepts such as multi-factor authentication and least privileged access controls. If keeping up with these changes is not in a business's core capability, third-party vendors are better suited to fill the gap.

Good operational practices (i.e., offline and encrypted backups of data at regular intervals, testing of backups and of disaster recovery plans, ongoing staff education, and reviewing on-going phishing and threat campaigns) are a must, but securing outside support for the strategy, plan, and services that are not core to your business is a cost-effective way to create a secure environment for your business and the sensitive data you are shepherding on behalf of others.

Compliance with HIPAA requirements and NIST best practices may be achieved by building everything from scratch, hiring new staff with experience and certifications, bringing in outside contractors help jump start and/or operate portions of the IT infrastructure and pipeline, obtaining environments and services that meet standards and are already certified, or a combination of these types of activities.

Conclusion

In summary, this White Paper suggests reducing cybersecurity threat risk by examining the Integrated System Development, Agile process, and CI/CD pipeline approach, reviewing and adhering to the proper federal standards, certifications, and compliance and following our recommended instructions for planning and securing infrastructure. The recommendations in this White Paper provide a practical set of actions to help organizations establish and improve their operational and security posture and reduce security threat risks to organizations holding the data and the population whose data is in their care.