EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

The Three Challenges Of Healthcare Data Security

This white paper outlines the state of security practices in healthcare organizations, common healthcare security setbacks, and potential long-term solutions for protecting PHI via HITRUST

Overview

The Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data Presented by Ponemon Institute, May 2016 "reveals that the majority of healthcare organizations represented in this study have experienced multiple data breaches" resulting from evolving cyber threats, preventable mistakes, and other dangers. With the industry scrambling to protect PHI, and the use of electronic communications on the rise, there is one word that dominates the conversation across healthcare IT departments: Security.

Security is the underlying issue that keeps IT professionals up at night, as they ask themselves "how can we keep our systems secure and our costs in check while supporting the growth of the business?" Adding to this already heavy burden on IT staff, systems, and resources is a broad range of compliance requirements from the federal government, state agencies, and the healthcare industry itself. For instance, on February 8th, 2016, five major healthcare payers issued a letter to their business associates (BAs) explaining the need for them to be certified to the robust, policy- and procedure-driven HITRUST Common Security Framework (CSF) within two years – as a minimum standard for doing business with them.

While there are many complex and related challenges around the topic of security, this paper looks at three specific issues, and sheds light on practical solutions for both now and the future.

Those challenges are as follows:

1. The industry is driving towards adoption of the HITRUST security framework. It is now a requirement for some business associates (BAs) and a governing standard for all who what to objectively demonstrate HIPAA compliance.
2. The volume and dynamic nature of environmental threats – to both PHI and business continuity – requires healthcare firms to have a flexible, evolving infrastructure with ever-improving security management.
3. The torrential waves of ransomware and other well-publicized cyberattacks are exposing sizable holes in traditional data backup strategies – escalating the need for employee education, and the adoption of isolated, off-site, and secure cloud backup solutions.

> *"I have gone out of my way to tell my board how difficult it is to protect information. This is so they fully understand that there is a non-zero likelihood of a breach."*
>
> **Omar Khawaja - Chief Information Security Officer, Highmark**
>
> HIGHMARK.

Compliance with HIPAA and HITRUST

Federal, state, and industry pressures are at an all-time high… Everyone who works in healthcare knows that HIPAA and other regulations are becoming more strict and enforcement is becoming more common and costly. In response to the tightening of these regulations, five major healthcare payers issued a letter to their business associates explaining the need for them to comply with the HITRUST Common Security Framework (CSF) within two years. Developed in collaboration with healthcare and information security professionals, the HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management. This mandate stems from the industry-wide drive to protect patient data and reduce the threat of PHI theft, privacy violations, or denial-of-service attacks.

In response to this announcement, Evolve IP participated in a seminar where leading healthcare CISOs discussed the new mandate and its impact on the subject of vendor management. Specifically, they addressed the operational benefits of adopting the HITRUST CSF and the mandate's impact on the many downstream business associates that provide services to the healthcare industry. The panelists included Omar Khawaja, Chief Information Security Officer of Highmark, Dave Snyder, Chief Information Security Leader of Independence Blue Cross, and Phil Curran, Chief Information Assurance and Privacy Officer of Cooper University Health Care. Below are some tips from this panel of experts:

1. Ransomware and the Increasing Volume of Cyberattacks

We are living in the digital version of the Wild, Wild West...

In addition to compliance concerns, many company executives and IT professionals are wondering how to protect against ransomware attacks.

The US Departments of Justice (DOJ) and Homeland Security (DHS) recently released a report that explains the need for ransomware protection and examines the scope and impact of recent cyberattacks. According to the DOJ report, the Internet Crime Complaint Center (IC3) has received nearly 7,700 complaints since 2005, which resulted in more than $57.6 million in ransoms paid and mitigation costs. Most ransoms were between $200 and $10,000; however, the growth rate of this threat is tremendous. In 2017, we have seen multiple global attacks (Wanna Cry and Petya) and the first ransom of $1 million in South Korea. The number of ransomware attacks increased by 6000% according to IBM! Further, it's important to keep in mind that many companies are reluctant to admit they didn't have adequate ransomware protection. So the statistics are only counting the publicly reported incidents.

There have been many well-publicized data breaches and ransomware virus/malware attacks that have crippled healthcare providers and their business associates.

Protection is as much about "infection response" as it is to "infection prevention". Below are some best practice considerations that can help ensure that your organization's business operations are protected in the event of an infection.

- **Create a Reliable Backup Process.** Create rapid, frequent system backups in a secure, offsite location.
- **Ensure Data Recoverability.** Backups can also be infected by the malware virus if not detected immediately after infection. Make sure your backups are isolated so they are protected and usable when needed.
- **Confirm Rapid Data Availability.** To expedite restoration, make sure you can access and act upon your backups immediately after an infection is identified.

Following the above best practices can limit your exposure to attacks, ultimately saving your organization time, money and bad PR.

2. Practical Guidance on HITRUST, Security & Compliance

HITRUST is a great framework for demonstrating HIPAA compliance – As HIPAA compliance is a subjective standard, rather than an agreed-upon minimum set of requirements, there is not currently a way to be qualitatively HIPAA-compliant. But HITRUST is the closest thing, offering a measurable baseline security certification. HITRUST goes beyond SOC II by requiring specific and rigorous security controls and requiring robust documentation of policies and procedures.

HITRUST is about long-term PHI security – Achieving HITRUST certification is just the beginning of a long-term process. BAs must continuously make corrective actions, follow and apply quarterly security updates, and take steps to build a culture of security.

We are still in the beginning stages – Covered entities will be driving increased use of the HITRUST CSF as a security standard and will require greater compliance efforts from the layers of business associates that support them. In essence, robust and quantifiable security is becoming a prerequisite for any BAs that want to be considered viable service providers to the industry.

Fundamentally, security is about people – Relying only on information security and IT teams for security efforts is a common IT misstep. All employees must be educated, evaluated, empowered, and enfranchised to create a secure environment. Senior management and the executives must also be highly involved to properly allocate time, money, and other resources that are required. Of course everyone, executives included, must then actually follow the policies which are set.

Certification is difficult, but has great value – HITRUST requires a demanding and time-consuming review of controls across the organization. However, a company with certification gains immediate recognition as a company focused on security.

There will always be risk, so be prepared – There is a non-zero likelihood of a breach. There will always be new risks and risks that are unmitigated. The key for covered entities is to make sure that they and their network of service providers are constantly improving by working on the most important things.

3. Continuous Infrastructure Security Demands

SMBs face a moving target with growing complexity

The demands to protect PHI and EMRs – starting with covered entities and flowing down through their network of business associates – require progressive security policies, procedures, and ongoing threat management. A compliant hosting backbone with actively managed security services – that can rapidly respond to daily monitoring requirements, security updates, emerging threats, or compliance changes – liberates organizations to better allocate their IT resources with a focus on key growth and business development strategies.

When considering the traditional challenges facing SMBs in the healthcare arena–limited staff, resources, and budget to address changing regulations and attacks– along with today's security and compliance challenges, a managed virtual private cloud can be a firm's best choice.

However, when you say "cloud hosting" to many IT professionals, they shudder at the idea of it. After all, the cloud is perceived by many as a risky, insecure, and immature environment with providers such as Amazon leading the charge. In reality, these perceptions are mis-perceptions when talking about virtual private cloud technology and environments that are actively managed and certified to the highest industry security standards. Healthcare organizations can benefit greatly from a virtual private cloud that offers an actively managed HIPAA-compliant infrastructure. In fact, an isolated, secure cloud hosting environment with geographically diverse and integrated backup and disaster recovery is the gold standard for small and medium sized healthcare companies.

The benefits of this type of environment include:

- **Greater Security.** A virtual private cloud with managed security offers a greater security profile than on-premise solutions–especially for smaller firms with limited IT resources. Physical security, power redundancy, multi-source connectivity, data encryption, and other physical features are available in premier data centers.
- **Higher Levels of Responsiveness.** Your environment is regularly monitored and updated to ensure the ultimate responsiveness to environmental threats. Reliable backup processes, data recoverability, and availability ensure that malware and ransomware are no longer the threat they once were.
- **Ensured Regulatory Compliance.** You maintain a consistent compliance posture despite evolving industry standards and practices. Hosting providers that are HIPAA and HITRUST certified ensure that your data management practices meet the stringent and constantly changing requirements of the healthcare industry.

> ***"As more and more entities get involved in regulating information, I see the covered entities, the people who are actually responsible for the data, getting more aggressive with their vendors on how they maintain the security and privacy of that data. I see us getting more aggressive. We have to deal with the FTC, FCC all these government agencies. That's what we need to be worried about. So we will be more aggressive with our vendors."***
>
> **Phil Curran - Chief Information Assurance and Privacy Officer of Cooper University Health Care**
>
> Cooper University Health Care

Evolve IP and Secure Answers for Healthcare

With HIPAA-compliant architecture that is audited to the HITRUST CSF standard and the only carrier-neutral data center engineered to the Tier IV Gold standard, the choice of Evolve IP is clear.

Evolve IP has deep expertise in partnering with the compliance-focused industries of healthcare and financial services as well as manufacturers and technology companies. As managed services and infrastructure experts, Evolve IP works with industry-leading technology providers like VMware to deliver the ultimate cloud experience to SMB's across the country.

Our clients can operate in a uniquely secure data center that is the first and only carrier-neutral collocation data center to be certified Tier IV Gold in Operations by the Uptime Institute. In addition, this data center meets and exceeds the standards of IEEE, ANSI, ASHRAE, 24/7, ISO 9001, SAS 70/SSAE-16, BICSI, and the Green Grid Association.

With 6 data centers across the country, we offer an unmatched combination of hardened infrastructure, geographic diversity, and technical skills.

Healthcare trusts Evolve IP for:

- HIPAA-compliant architecture that is audited and certified to the HITRUST Common Security Framework (CSF) standard
- Managed services that provide flexibility, scalability, intelligence, and a 24/7 response team—in a consumption-based model for a single monthly fee
- Partnerships with leading software and hardware technology firms to deliver high-quality business solutions
- A Tier IV data center that is the only one of its kind in North America
- Geographic redundancy between east and west coast hosting sites and built-in disaster recovery
- Industry thought leadership and educational programs
- Extensive cross-industry IT infrastructure experience
- Hybrid cloud flexibility, enablement, monitoring, and management
- Hosted PBX and call center solutions
- Sales support from certified solution engineers
- Unsurpassed professional services expertise
- 24/7/365 support

About Evolve IP

Evolve IP is The Cloud Strategy Company™. Designed from the beginning to provide organizations with the ability to deploy both cloud computing and cloud communications onto a single platform, today, nearly 200,000 users rely on Evolve IP for services like disaster recovery, contact centers, unified communications, virtual desktop services, IaaS and more. With deployments across the globe, Evolve IP provides cloud services in virtually every industry with specializations in the healthcare, finance, veterinary, retail, legal, and insurance verticals.