ClearDATA
SECURE • HEALTHCARE • CLOUD

9 Common Security and Compliance Risks

And What You Can Do to Overcome Them

About the Authors

CHRIS BOWEN

Chief Privacy & Security Officer and Founder, ClearDATA, CISSP, CCSP, CIPP/US, CIPT

Chris is responsible for ClearDATA's defense-in-depth approach to cybersecurity and privacy by design. He manages the risks and business impacts faced by global healthcare organizations, with a specific focus on cyber threats, privacy violations, security incidents, social engineering attempts, and data breaches. As one of the leading experts on patient privacy and PHI security, Chris has authored dozens of articles and is a frequent speaker at healthcare industry events.

MATT FERRARI

Chief Technology Officer, ClearDATA

Matt has been one of the most influential leaders in cloud computing since his earliest days in the industry, starting at Hosting.com where he architected and built the company's award-winning public cloud platform. He joined ClearDATA in 2014 and a year later, launched the first healthcare-exclusive AWS cloud platform, focused on automation and compliance. As CTO, he leads the teams that are integral to the company's rapid growth: Product Strategy/Vision, Product Management and Product Development, contributing to 100%+ growth for the past several years.

Healthcare professionals across the globe trust the ClearDATA HITRUST- certified cloud to safeguard their sensitive data and power their critical applications. We offer our customers the most comprehensive Business Associate Agreements (BAA) in the industry, combined with market-leading healthcare-exclusive security and compliance solutions. Our innovative solutions help protect our customers from data privacy risks, improve their data management, and scale their healthcare IT infrastructure, enabling our customers to focus on making healthcare better by improving healthcare delivery.

Healthcare Security Incidents and Breaches

According to the ITRC Data Breach Report 2017:

Healthcare - 2nd biggest contributing industry to overall breaches in 2017 with

334 breaches

The Identity Theft Resource Center (ITRC) has been tracking security breaches for more than a decade and has said in their 2017 ITRC Data Breach Report that healthcare was the 2nd most significant contributing industry to overall breaches with 334 breaches. The industry was the target of ransomware, hacking, skimming and phishing attacks as healthcare records become increasingly desirable for those looking to commit identity theft.

Data breaches are crippling to any business, but are extra hard on healthcare organizations, considering the vast amount of sensitive information consumers trust them with and the irreparable damage to reputation that can follow a breach. Healthcare entities are held to the highest trust standards, and face increasing federal and state penalties and fines when breaches occur.

At ClearDATA, we're providing innovative solutions that address compliance, privacy, and security, enabling the healthcare industry to focus on healthcare delivery instead of data risks.

By moving to the cloud, our customers gain expansive resources for collaboration to help improve outcomes and compliance as we protect them against the latest, ever-evolving threats of a data breach.

In our work we see similar security and compliance risks surface over and over. In this e-book, we'll look at the top nine, and help you understand what you can do to overcome them at your healthcare organization.

Sources:
Identity Theft Resource Center. "ITRC Sponsors and Supporters ." ITRC, Identity Theft Resource Center, 12 June 2018, www.idtheftcenter.org/Data-Breaches/data-breaches

9 Common Security and Compliance Risks

- Data Sprawl
- Unmanaged Data Flows
- Misconfiguration
- Incorrect Identity Management
- Role Drift
- Vendor Due Diligence
- Lack of Agility
- Shadow IT
- Lack of Knowledge Around Cloud Security

Data Sprawl

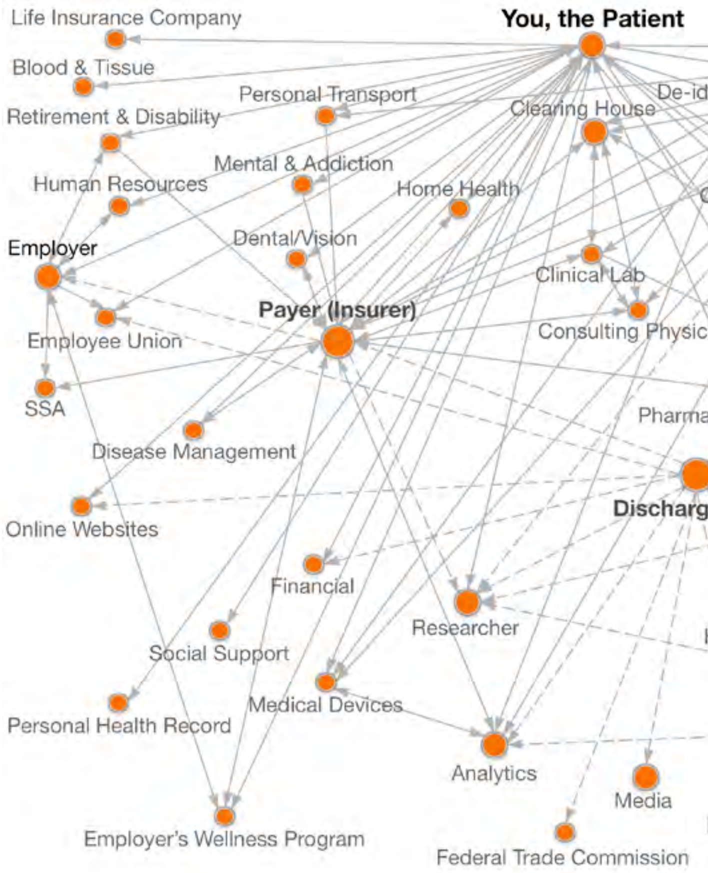
Data sprawl is a growing concern as more and more people use more and more devices from an increasing number of locations. It's difficult for a healthcare organization to know where their data is, and until you know that, you certainly can't protect it.

What to Do:

Begin by making sure you have strong data protection policies in place. You'll need them once you succeed in locating your data, which is the first action after making sure your policies are in place and updated. Whether you use new technology tools or a more traditional interview and discovery process, identify what data you have and understand where it lives. You may have databases in use as well as retired databases; you may have private or hosted data centers, private or public cloud instances. Choose a discovery tool or set of tools that can provide a single view into data of any type, regardless of the storage repository. Then, classify your data. Not all of it will require the same level of protection. You'll be better prepared to build your most robust safeguards around the data that needs the most protection by working from a clear and consistent classification system. Once you've classified your data, work to manage your risk. Keep management teams informed of the efficacy of monitoring systems and ensure security operations are aware of and working to remediate any detected violations. Customizable dashboards and reporting mechanisms can provide visibility 24/7 as you incrementally improve.

Unmanaged Data Flows

Tied closely to the previous risk is unmanaged data flows. Healthcare organizations have not historically been tremendously successful at mapping the flow of data into, within and out of an organization. It's no wonder when you consider this visual (above) that demonstrates data flow provided by The Data Privacy Lab at Harvard University in the DataMap Project. (https://thedatamap.org).



What to Do:

Data drift and unmanaged data flows are in many ways unavoidable, but you can work to make it a more managed flow by implementing tools and processes to map your data flow, and to detect when unexpected changes occur. Automation can aid much of the change detection in the cloud. Once you build out instrumentation or utilize tools to visualize how your data flows, then you can assign roles and responsibilities. Document who is responsible for managing each piece of data as it flows through and out of the organization. Ultimately, you'll do a better job of tracking your data flows, and in the process, you find inefficiencies that you can correct and harden inside your environment. It's probably you'll not have 100 percent visibility to really understand where all of the data is going, so plan your systems, make sure your architecture references reflect those data flows you can identify. Instrumentation can keep you informed and a step ahead of inevitable changes and mutations in the data as it flows.

Misconfiguration

Anyone working with healthcare data has seen or read about misconfigurations that led to data security incidents and breaches. Often well-intentioned people make configuration changes without understanding the downstream effect of those changes that can leave your organization damaged. It may be simple bucket changes that expose top secret files, or accidentally opening a firewall rule. Often it is not the data center or public cloud that is going to jeopardize your organization; it's the human user whose operations create a vulnerability that can lead to the leaking of millions of records.

What to Do:

Ensure your organization enforces rigor around change management. Undisciplined change management is the genesis of so much of misconfiguration. Exposing changes in your environment to an established change management process is critical. In addition to proper change management, also document what the system should do and who owns the change process. The secret weapon is automation. There are ways to automate steps in IT that eliminate the human error factor and misconfigurations will rapidly decline. ClearDATA has implementation automation in the public cloud for its customers to make less work for them, and significantly reduce the chances of misconfiguration. Healthcare organizations investing in automation will get timely alerts and notices when something is amiss and in many cases before a human might have detected it. Think about a pilot flying a plane. He or she has a checklist they have to go through item by item, every single time. That's how you have to think about automation, start with the list of processes likely to potentially encounter errors and investigate how can you automate that with healing or remediation along the way.

Incorrect Identity Management

Fast-growing organizations are often focused on speeding time to market and overlook identity access management, leaving themselves prone. Often, employees of an organization will have access to more things they should, and certainly more access than they need to do their job well. For example, subscriptions may have shared user IDs or credential sharing.

What to Do:

Incorrect identity management is not hard to fix with policies and processes in place to monitor who has access to what, and why. Start with a principle of granting the least access possible for the person to do their job effectively. Limit admin roles and review them frequently to ensure each person still needs higher level access and privileges. Don't grant access based solely on title or job description. Create individual users, not shared credentials. Have a policy and password for strong password configuration. Enforce your password complexity requirements to protect against brute force login attempts, considering a policy for 14 characters or more, one letter, one character and one number as one example. A best practice is to create a control for password expiration and refresh every 90 days. Closely manage permissions with groups. Have regular checkins to ensure any changes to the data flow still require the same access. IT departments need to rotate security credentials and keys regularly to ensure data cannot be accessed with lost or stolen keys. Another best practice is to deactivate any credentials that are not in use after 90 days. A HITRUST certified managed cloud provider can provide you with additional advice to shore up this risk and protect your organization.

Role Drift

Closely related and sometimes overlapping with identity access management is role drift. Especially in technology start-ups, positions and roles change frequently based on company objectives and quarterly goals. Everyone thinks about onboarding but often overlooks periodic changes in duties and off boarding to ensure the removal of access.

What to Do:

Your policies need to document and reflect how you are ensuring the minimum access possible. Reviewing roles in quarterly formal meetings is a best practice. Harden your onboarding and your offboarding process. So often departing employees leave an organization and retain access they should not have. Set and adhere to strong policies for this. Microservices can provide a great solution to the common role drift problem. If you have a service account that has a role like accessing a database or processing something inside a database, you don't need an admin role for that account, you can use microservices to carry out that function. The world is quickly moving toward microservices and ultimately serverless models. Your managed services provider can show you how to make the microservice call a single API call for a sole purpose. This strategy mitigates risk and makes sure any role only fulfills the service call that you need it to, nothing more and nothing less.

Vendor Due Diligence

Anyone responsible for vendor selection has probably been guilty once of cutting corners and selecting a vendor solely on price or the appeal of the product. Cutting corners here can leave you disappointed, and it can also lessen your ability to secure, scale and grow your business. Based on the need, a vendor may be one of your strongest strategic partners and allies, or they may hold you back. Not all cloud vendors are created equal.

What to Do:

Do your due diligence. The good news is you don't have to create an RFP from scratch every time you need to select a vendor. Industry analysts have done a lot of the legwork for you and also provide beneficial repeatable due diligence documentation. For example, let's assume you're picking an intrusion detection vendor. An analyst has likely documented what ten key criteria you need. The product being the right price doesn't mean it's the right product, so always map it back to your requirements that you have articulated before you begin your search, and make sure it does what it says it is supposed to do. One of the ways ClearDATA builds and deploys new products and features is by acting on feedback we've received from customers during due diligence. Also, ask about their security risk assessment. What kind of risks exist inside the vendor's security environment. What have they done to button up from a rigor and process perspective?
It comes down to diligent contracting. At ClearDATA, we use a very detailed RACI matrix for who is responsible, accountable, consulted and informed for every part of the vendor process, from the service level agreement to who is monitoring the environment - and it's all in the contract agreement. Repeat your review process regularly to make sure your vendors are still doing what they are supposed to be doing.

Lack of Agility

Now more than ever, healthcare organizations need agility to scale their businesses and speed their time to market. Agility is difficult when they find themselves shackled with antiquated legacy systems, capital expenses and time and energy spent focusing on maintaining hardware ordering and inventory levels and capacity. The need to order a 100-foot-long internet cable for a data center delayed one CIO's project for several months. Managing IT resources outside the cloud can actually obstruct the process of achieving business growth objectives.

What to Do:

Use the cloud for the cloud, it has been built with agility and scaling baked into the system. You need to have vendor agreements in place before migrating. Understand your service level agreements and make certain your vendor partner can take on your security and compliance regulations as you make the move. Security and compliance for health data require a deep healthcare expertise given healthcare's ever-increasing compliance regulations and growing security threats. Create a cloud governance model with your managed service provider and use it, but with some flexibility. Whenever possible, take advantage of the native cloud tools and the extensive DevOps talent that are built around compliance and agility in the public cloud, rather than trying to DIY and build from scratch with your intellectual property as this will slow you down. The three main public clouds are releasing new features almost daily that can help grow and manage your business provided you have the security and compliance guardrails in place, such as the automated safeguards a healthcare exclusive managed service provider builds into the environment for you.

Shadow IT

With the growing adoption of apps and mobile devices, employees in all sectors are using apps that are not sanctioned by their IT departments, with studies pointing to numbers as high as 70% of employees using shadow IT. Shadow IT makes your organization prone to hackers yet the average healthcare organization runs about 900 services – more than any IT department knows is in use.

What to Do:

Begin by stating a strong policy about shadow IT and be clear what will and what will not be tolerated. Bear in mind, however, that most shadow IT users are doing to so to improve their productivity so be open-minded and look at what they are using while remaining firm about them conforming to accepted change management policies and practices. Embrace that the cloud is changing the world of shadow IT. You can use native tooling like the ability to look inside of your own public cloud account where you can identify subaccounts to determine who is spinning up or down resources and tag them. Some organizations charge back by tying their cloud usage back to their budget to pull these users and departments out of the shadow. Another benefit to the cloud is the more shadow IT users adopt the cloud, the less you will have to worry about third-party vendors – your employees can work inside the approved cloud instance with security measures in place. And, get involved with business units outside of the IT department to see what they are doing and why, as innovation doesn't only happen in IT.

Lack of Knowledge Around Cloud Security

This problem is getting worse as the healthcare cloud is increasingly embraced. Approximately 35% of the cloud services are commissioned without the involvement of IT, leaving cloud security organizations inside these companies with a blind spot. Additionally, many IT organizations lack mature talent in understanding the big picture around cloud security, complicated by the fact many public clouds have dozens of different services and varying cloud security models all of which continuously have rollouts of new features and functionalities.

What to Do:

Only partner with someone who is committed to securing your healthcare data in the cloud. Find an organization that is facing the DevOps staffing challenge by investing in their talent and making sure their team is cloud certified in addition to the company's own HITRUST certification. Pick a partner who is healthcare exclusive and HIPAA compliant. Then, step outside your comfort zone a bit and ask them to help educate you on the cloud. They should partner with you leading you into a discovery process that builds expertise in your team, creates a more independent ability to innovate in the cloud while remaining secure and complaint and opens a culture of inquiry to explore and adopt all the cloud is offering for agility and scaling. As mentioned earlier, do your due diligence, audit your cloud provider as they will become one of your most important strategic partners.

To learn more about ClearDATA's healthcare-exclusive expertise

CONTACT US