NOVEMBER 15, 2021

Healthcare Data Security: Why It Matters

BY KELLY DYER

Healthcare Data Security

Today, electronic healthcare data exists at every point along a patient's journey. So frequently is it being processed, accessed, and shared between multiple providers, that we'd be forgiven for forgetting the highly sensitive and confidential nature of this information, and for taking data security for granted.

Healthcare data not only contains medical information, but also provides possibly the most comprehensive amount of personally identifiable information (PII) on an individual, making it an attractive target for cybercriminals. PII, such as full name and date of birth, current and previous addresses, contact numbers, financial details, are all vulnerable to being exploited by hackers.

Healthcare Data Explosion Vs Retention

When you combine the quantity of healthcare being generated with the length of time it needs to be stored, it is no surprise that protected health information (PHI) and PII falls under the strictest security legislation. To give you an idea of scale, it was predicted that in 2020, **over 2,300 exabytes* of new healthcare data** would be generated globally, compared to just 153 exabytes in 2013! [*1 exabyte = 1 billion gigabytes]

Compounding the challenges of **healthcare data** management is retention. In the USA, HIPAA legislation requires medical records to be retained for six years, from the time it was created or when it was last in effect, whichever is greater. However, a number of parameters can influence this, such as frequency of appointments, insurance contracts, potential or pending lawsuits, and individual state laws. The suggested **medical record retention between states** can range from five to 11 years for adults, and for minors as much as 30 years from birth.

It's not just the healthcare providers having to process and retain **sensitive data**, it's also the health insurance companies. As the need for **telemedicine** came into its own during 2020 the American Medical Association (AMA) finally released **2020 CPT® (current procedural terminology) codes** for virtual consultations. This gave the green light for patients and physicians to process compensation or insurance claims for virtual appointments, again all managed on the cloud.

It's no wonder that with this exponential rise in data volume and associated storage requirements, healthcare providers have gradually moved from on-premise servers to a cloud environment. And with the rapid demand for an increase in telehealth during the pandemic, healthcare cloud computing is predicted to keep growing at **18.1% CAGR by 2025**, now with **more than a third of providers choosing a hybrid approach**.

Healthcare Data Security On The Cloud

Even though medical records are no longer physically present or physically in our control, as the digital evolution transformed healthcare life sciences over the last few decades, data **security has always been the top priority**. Cloud-based solutions for healthcare professionals and organizations have enabled them to retrieve, process, share, and analyze vast amounts of data at the touch of a few buttons, revolutionizing patient care, improving outcomes, and accelerating medical research.

However, protecting data on the cloud from unsanctioned access or corruption has never been more important. Implementing robust **security measures will mitigate against the risk** of potential financial penalties, data recovery costs and upheaval, loss of trust and confidence, or irrevocable damage to an organization's reputation.

Guidance on how to comply with data security regulations can be drawn from the Health Insurance Portability and Accountability Act (HIPAA) federal statute. HIPAA rules and regulations provide a specific component for dealing with electronic PHI, known as The Security Rule, setting out administrative, physical and technical safeguards in order to be compliant.

Implementing Cloud Data Security

The burden of responsibility for *technical* safeguards should largely fall to cloud technology providers, since this must be, without question, their level of expertise. If the cloud solution partner is also HIPAA-compliant in their own right, even better! In this way, healthcare providers can focus on their patients, while their cloud solution partner concentrates on keeping their data and infrastructure secure.

Having migrated to the cloud, the most up-to-date cloud services for **cybersecurity** can be seamlessly deployed, with the ability to integrate new regulatory compliances and policies, as and when they become available. And all this while provisioning for scalability and reducing total cost of ownership.

When contemplating what cloud security services to implement, it's helpful to consider it in terms of **Amazon Web Services** broad headings:

- **Compliance: does the cloud technology adopted adhere to regulatory policies?**

Any cloud technology being used to manage healthcare data must adhere to HIPAA and GDPR regulations and policies. This should serve as the baseline in helping to mitigate and **manage risks**, and in addition provide the necessary functionality for continuous and/or real-time auditing and reporting purposes.

- **Safeguards: how will the infrastructure be protected?**

There are cloud services available that will provide a first defense 'shield' against potential cyber-attacks. Not only that, certain 'rules' can be enforced that will proactively respond. For example, protecting data from unauthorized access through encryption *plus* automatic encryption key replacement.

- **Threat detection: will the technology detect and warn of potential breaches?**

A big part of being able to detect potential threats or breaches before they actually happen, is the ability to monitor behavior and track user activities.

- **Actions: what happens if and when a threat is detected?**

As well as analyzing and detecting potential security issues, today's smartest cloud technology includes the ability to automatically troubleshoot and initiate next steps. With **machine learning** and statistical analysis, root causes, and what caused it in the first instance, are rapidly identified and next steps initiated.

- **Access: how can unauthorized access to data be prohibited?**

Obviously, the level of cloud security services deployed can go a long way in limiting access, but organization-wide education and awareness is also key. Implementing technology with robust multi-factor authentication, that can restrict sharing permissions, and flexibility to set user-profile clearances, all helps to ensure specific PHI and PII are accessible by authorized users.

Bottom Line

While cybercriminals find more creative and devious ways to get access to protected data, it's vital for a healthcare organization to continuously review and assess its levels of security. Cloud service providers can work strategically with CIOs and CTOs to maximize healthcare data security, leveraging cloud technology that provides maximum protection while also meeting regulatory compliances. Maintaining trust and confidence that our sensitive and confidential healthcare data on the cloud is safe, means we should never get too complacent. With the help of dedicated cybersecurity expertise trust and confidence can be achieved, deploying the very latest security software so that nothing is left to chance.

By Kelly Dyer

KELLY DYER

CEO and Co-founder of SourceFuse Inc., Kelly is a life-long entrepreneur and technologist, with over 23 years of experience in identifying challenging problems and opportunities that can be solved with software and innovation. Kelly is passionate about product development and disrupting industries through better use of technology, working with start-ups and enterprises alike.

Kelly co-founded SourceFuse in 2006, a digital product and technology development organization that is transforming the way today's most successful companies develop breakthrough roadmaps leveraging cloud-based technologies, designing, building, and managing software and technology products and solutions from concept to implementation.

Prior to establishing SourceFuse, Kelly founded Inventory Source in 2003, where he remains today as an executive board member, a company that provides custom data solutions and automation directly for new and existing retailers' websites on a variety of platforms.

With his wealth of technological experience and enthusiasm for digital transformation, Kelly currently has key advisory roles at several startups as Investor/Advisor, and an Advisory Board Member in the Connolly Center for Entrepreneurship at Washington and Lee University. In 2015, Kelly also founded the Jax Tech Group, creating a vibrant networking community for like-minded technology experts and enthusiasts in the Jacksonville region.

Kelly holds an MBA from Duke University – Fuqua School of Business, NC, and a degree in Computer Science and Economics. Based in Jacksonville, FL, Kelly is an avid surfer, golfer, snowboarder, and global traveler.

WEBSITE

SPONSOR PARTNER

getsmarter® with edX®

Explore top-tier education with exclusive savings on online courses from MIT, Oxford, and Harvard through our e-learning sponsor. Elevate your career with world-class knowledge. Start now!