PRIVITAR

Expanding Data Use In Healthcare with a Privacy First Approach

Patient information and healthcare data at large is often locked away, or destroyed before use can even be considered. This has been for good reason as legislation like HIPAA has introduced new data regulations, and healthcare has taken the brunt of the increase in data breaches, accounting for 25% of the total across all industries.[1] These breaches have resulted in compromised medical information for 26% of US consumers.[2] This headache continues as health records are the most valuable type of personal information available - estimated at $408 per record by IBM's Ponemon Institute. The value of data and prevalence of breaches has reasonably caused many organizations to lock data away, making it unavailable for analysis. The most disappointing part of this reality is that this data could be leveraged to help doctors and pharmaceutical companies combat disease and improve patient outcomes.

Implementing Privacy for Patient Protections

Patient medical records are being compromised at an increasing rate, and the leaks are coming from across the care continuum. Major data breaches have now been attributed to every major part of the healthcare system with hospitals, pharmacies, and insurers all being victims of nefarious actors - both internal and external. Patients that are the subject of a breach typically experience hardship as a result, with 50% of victims[2] experiencing medical identity theft that was used for fraudulent activities like billing care or filling prescriptions. The average out of pocket cost to a victim of medical identity theft totals $2,500.[2] And unlike banking or credit costs, healthcare provides little to no financial protection for these victims.

Accompanying the increasing breach numbers is also increasing regulation. HIPAA and the GDPR are the latest attempts to restrict and enforce how personal information is used. HIPAA's specific focus on healthcare has compounded the headaches associated with managing Personal Health Information (PHI). Organizations who collect this data are faced with protecting a highly valued and regulated asset, a challenge that is not easily solved in today's highly distributed IT and healthcare environments.

As healthcare organizations have considered how to protect this data the typical approach has been to increase cybersecurity controls. As a result pharmaceutical companies, healthcare providers, and insurers alike have implemented technology and policies to lock data down, restrict access and limit usage. Unfortunately, this approach has been unable to reduce the impacts of breaches, because it is an incomplete strategy. Locking data away except for the most privileged access leaves it vulnerable when it is in use. This means there will always be points of failure that can be exploited, whether they are inside or outside of your organization.

The Call for Medical Data Democratization

It has long been the prediction of healthcare futurists that, when data being harvested from the clinical environment is combined with the analytical power of modern computing, we will unlock new treatments and be able to dramatically improve the patient experience. A requirement in this depiction of the future is that data can be shared and leveraged across providers for a broad range of studies. We are working towards realizing this future with disciplines like healthcare informatics

1. Thales Data Threat Report by IDC. 2. Accenture Survey, 2017

and population health analytics becoming integral parts of the healthcare system. These new sciences rely on the quality and availability of data. However, the promise of these disciplines remains out of reach, because researchers and providers spend the majority of their time waiting for data or, worse, de-identifying it and preparing it for use.

The democratization of any data sets that contain PHI requires a complete data protection approach in order to protect patient privacy and respect regulations like HIPAA. Data masking and field level de-identification are not new concepts in healthcare. Developers have been writing custom scripts for years. This approach has been sufficient for small, local efforts. As the need for data expands, there is an equal need to provision data for use faster, creating a problem at the intersection of manual process and traditional security controls. This is where a data provisioning platform that enables privacy by design can make all the difference, by quickly preparing data to be used in a safe manner.

When health data scientists, healthcare informatics professionals, and pharmaceutical scientists alike can get their hands on the right data, it can dramatically accelerate results and how resources are deployed. Data has changed treatment plans for patients with multiple conditions, altered how providers think about proactive care, and transformed how outcomes and care are assessed across all areas of treatment.

Mitigating the Risk of Healthcare's Digital Transformation

The healthcare environment provides an enormous opportunity for data collection and analysis that can change how people live their lives. The flip-side is that it is the most sensitive data available. As organizations continue to evaluate how to broaden the usage of data, it is critical they contemplate a data provisioning strategy that will infuse their data sets with privacy while maintaining analytical utility. This balance is essential in forming a complete data protection strategy that properly evaluates how to protect data from the time of collection all the way through to usage and ultimately deletion.

Privacy has been built into almost every aspect of the modern health system, and that needs to extend to data in a more meaningful way. As teams share and utilize data in more powerful ways, it becomes clear that they need a platform that can manage data de-identification for a wide range of scenarios. The variety of scenarios in healthcare dictates the need for a platform that can run different de-identification techniques in any combination across the data dependent on the use case. The right platform also makes the privacy protected data available for access in a secure environment to internal and, optionally, third party researchers and providers. And it fully manages the data lifecycle by eventually destroying it based on configuration. In the event of a breach the right platform will not only have protected each individual's privacy within the data itself, it also provides traceability enabling better tracking and management of data that appears somewhere it shouldn't.

Organizations with a well designed sensitive data management strategy will not only be poised to capitalize on their data, they will also be in the best position to protect their sensitive health information. This position of strength will improve treatments and outcomes while building trust in the community as they are recognized as a good steward of data. These organizations will be in a better position to mitigate risk, as data that has been declared available for use will be protected. And in the event of a breach, data traceability will give them insight into where it occurred, allowing for clearer communication and, ultimately, a more positive public perception.

Privitar for Healthcare

Data privacy has long been a focus of healthcare and Privitar provides a data privacy solution that enables complete management of sensitive health information. Making the Privitar Data Privacy PlatformTM an integral part of your data pipeline will enable application of consistent Privacy Policies that allow your organization to safely utilize patient data in a compliant manner.

> De-identification. Privitar provides a complete range of de-identification techniques to preserve data privacy. De-identifying patient data will complement typical security technologies by extending protection to data in use, ultimately allowing for broader consumption.

> Automation. Privitar enables Privacy Policies to be defined centrally and applied systematically using metadata from Privitar and other data pipeline systems. This design accelerates the data provisioning process at scale - decreasing time-to-data and enabling compliance with laws like HIPPA, GDPR, and PIPEDA.

> Scalability. Privitar includes a comprehensive set of RESTful APIs that enable organizations to automate and orchestrate their data de-identification and provisioning processes. Programmatically configure policies that ensure underlying patient privacy is protected across all use cases.

> Watermarks. Privitar Watermarks are unique technology that enable end-to-end traceability of sensitive data. Watermarks allow tracking and management of full data provenance.

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136
US +1 857 347 4456
w: www.privitar.com

PRIVITAR

@PrivitarGlobal

www.privitar.com