The Heart of Healthcare Data Security- De-Risking Test and Production Environments

Abstract

The growing maturity of Electronic Health Record (EHR) systems and healthcare information exchanges (HIE) and the digitization of health care is driving down costs and improving the quality of care. However, the increasing interoperability and access to Protected Health Information (PHI) and Pelba itnedI yllanosre Information (PII) is accelerating the risk of data breaches. A unique persona-based approach that leverages a secure repository to effectively assess, remediate, and monitor data risks in the test environment can help healthcare companies secure the production environment and lay the foundation for enterprise-wide data security.

According to a study by Ponemon Institute, the cost of a data breach to healthcare organizations was $363 per capita, which is far higher than in any other sector.

91% of healthcare companies reported at least one incident in the past two years, at a total cost of $6 billon, with $2.1 million spent on an average incident.

The consequences of a security breach include wastage of time and resources, cost of reporting the incident to federal and state authorities, regulatory fines and class-action lawsuits, cost of fixing IT systems, disruption of operations, and long-term damage to reputation.

A Key Business Implications of the Data Breach Epidemic

Stolen healthcare credentials sell for 10 to 20 times more than stolen credit cards on the black market[1]. Not surprisingly, lucrative patient information residing within poorly protected applications, databases or networks, make healthcare organizations natural targets for security attacks.

Apart from cyber crime, lost or stolen devices, non-centralized hospital systems, disgruntled employees, and shared computing all pose potential security threats. Ignoring these securitdna ,lagel ,laicnan   tnac   ingis ot dael nac sksir y reputational losses.

A ot nalP eraC eht gnin   eDvoid Security Risks

Healthcare organizations are collecting, managing, analyzing, and sharing an increasing amount of electronic data. Much of this includes PHI and PII from various sources including transactional systems such as enrollments, claims, billing and patient portals, as well as integrated services such as medication adherence and pricing. The widespread distribution and access to PHI through a growing array of Internet-connected devices, tools, and sites makes it even more challenging to secure data.

To stay compliant with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, healthcare organizations must continually monitor their physical, administrative, and technical security policies to safeguard sensitive patient information.

One area that is often overlooked is the widespread use of sensitive patient data in healthcare application development. This practice exposes organizations to the risk of non-compliance and can lead to the mismanagement of PHI and PII.

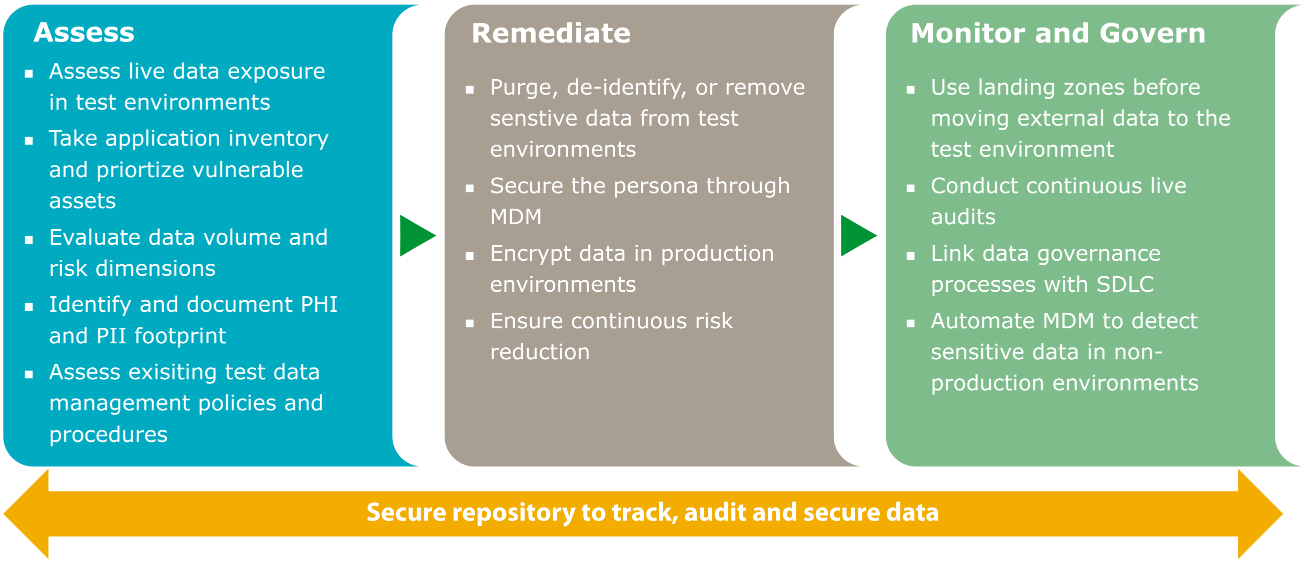
Large healthcare payer organizations typically have 2500-4000 applications and several membership and claim engines. In addition, a growing number of external services make the data and application landscape more complicated and vulnerable

Improving Test Coverage to Prevent Data Breaches

Compliance regulations and security best practices require organizations to inventory and classify their information assets. However, fast paced development cycles push rapid technological innovation through the IT departments of healthcare companies, putting sensitive data at the risk of being overlooked or mismanaged.

This problem extends beyond the production environment to the testing environment as well. Testing forms an integral part of a successful new system roll out and testing systems have grown in complexity to address all functional groups and potential production scenarios. Often, copies of production or actual patient data are used to populate the test environment, creating security loopholes.

Securing healthcare data requires identifying and mapping the organization's PHI footprint in both production and test environments, and understanding how the data can be compromised. Once sensitivti ,de itnedi neeb sah noitamrofni e should be masked with the help of foolproof data de- .noitac itnedi



Assess

- Assess live data exposure in test environments
- Take application inventory and priortize vulnerable assets
- Evaluate data volume and risk dimensions
- Identify and document PHI and PII footprint
- Assess exisiting test data management policies and procedures

Remediate

- Purge, de-identify, or remove senstive data from test environments
- Secure the persona through MDM
- Encrypt data in production environments
- Ensure continuous risk reduction

Monitor and Govern

- Use landing zones before moving external data to the test environment
- Conduct continuous live audits
- Link data governance processes with SDLC
- Automate MDM to detect sensitive data in non-production environments

Secure repository to track, audit and secure data

ARM is a unique persona-based approach for securing the test environment.

The ARM Framework for Fortifying Data

The Assess, Remediate, and Monitor (ARM) framework is a highly effective tool to prioritize, safeguard, and monitor vulnerable data and applications.

Preventive Care for High-Value Targets in Production

The ARM framework, used to drive test data management efforts, is also valuable for driving cyber security initiatives focused on data security. Often, it is not lack of technology that slows down cyber security efforts in the production environment but lack of clarity on how to minimize risk systematically. The PHI footprint collected in the non-production enti erehw ,derots si atad tahw se   itnedi tnemnoriv is stored, and the volume of that data. This allows production data security efforts to focus on high value targets as the priority.

Cyber Security Initiative	Opportunities for Improvement
Application Security	Prioritize applications with protected data in application security reviews, application firewall programs, and entitlement reviews.
Database Security	Prioritize databases with protected data in database activity monitoring, privileged user management, and database encryption programs.
Server Security	Prioritize servers hosting databases and applications with protected data in privileged user management Programs.
Vulnerability Management	Prioritize servers and databases hosting protected data when vulnerabilities are found. Prioritize patching and database hardening efforts for databases and servers hosting protected data.
Data Loss Prevention	Utilize master data for protected data to decrease false-positive identification of data loss events.
Governance, Risk and Compliance	Feed protected information into GRC tools and processes for enterprise risk assessments.
Security Information Event Management	Prioritize applications and databases to feed security events to the Security Operations Center. Use inventory of applications and databases with protected data to prioritize security alerts and speed up responses and notifications.

Leveraging the ARM framework in the production environment

Long-TP a fo st   eneB mreersona-Based Approach

The persona-based approach adopted by the ARM framework ensures that development activities take place quickly and securely in test environments, with minimal disruption to business release cycles. Some of the kMRA eht fo st   eneb ye framework are:

- **Improved regulatory compliance**

Organizations can improve compliance through comprehensive de-identification and removal of sensitive data from test environments, as well as better data audit and governance.

- **Reduced risks**

The ARM framework offers greater clarity on prioritizing risks. In addition, remediating test environments and securing live data significantly lowers business risks arising from data breaches at an enterprise level.

- **Maintenance of application integrity**

De-identification of data ensures compliance while supporting production-class testing, without hindering application functionality.

- **Accelerated testing**

The framework supports rapid testing that is aligned with key elements of the SDLC. It also helps improve productivity through automation of data masking, especially when provisioning new test environments.

- **Consistent data masking**

With multiple applications running on different databases, PHI and PII must be masked in a consistent manner across applications. The ARM framework recommends a standardized dna elbalacs si taht atad fo noitac   itnedi-ed ot hcaorppa .sdnamed erutuf teem ot elbixe

A large US healthcare payer eliminated 65% risk at half-time with zero to minimal disruption to their business and IT release cycle.

Conclusion

Healthcare security breaches highlight the fact that healthcare data holds value not only for healthcare organizations but also for unscrupulous entities. These incidents underscore the need for a new approach to data security, as it is no longer enough to rely on encryption, data leak prevention, access management, and other information security technologies. Organizations must leverage a holistic combination of process change, leadership, and technology implementation to secure both production and test environments.

Robust healthcare data security goes beyond preventing data breaches. It creates superior business value by enabling healthcare organizations to adopt new business models and technologies rapidly, paving the waseicneic   fe decnahne rof y and competitive advantage.

Footnotes

[1] Network World, Anthem hack: Personal data stolen sells for 10X price of stolen credit card numbers, February 2015, Accessed July 2015,

http://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

About The Authors

Viswanathan Ganapathy and Daniel Logan.

Contact

Visit TCS' Healthcare Business unit page for more information

Email: healthcare.solutions@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model^{TM}, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com