

Test Coverage vs Liability - A Healthcare TDM

by Shashi Kiran KV



The growing maturity of Healthcare IT and the digitization of healthcare is improving the quality of care and driving down costs. Nevertheless, the risk of data breaches from the ever increasing interoperability and access to Protected Health Information (PHI) and Personally Identifiable Information (PII) is accelerating. The consequences of a security breach include disruption of operations, cost of fixing IT systems, cost of reporting the incident to federal and state authorities, regulatory fines and class-action lawsuits to business and credibility loss.

Healthcare data breaches

- Costed the industry as much as \$6 billion, with an average organization cost of \$2.1 million per breach¹.
- 67 American healthcare organizations reported an average of 2.4 breaches annually during the last 2 years².

¹Breaches Cost Healthcare \$6 Billion Annually:

<https://www.healthitoutcomes.com/doc/breaches-cost-healthcare-annually-0001>

² Data Spills Cost U.S. Hospitals \$6 Billion A Year:

<https://www.forbes.com/sites/andygreenberg/2010/11/08/data-spills-cost-u-s-hospitals-6-billion-a-year/#ce811e17a774>

Test Coverage vs Cyber Liability Coverage

Data compliance standards (HIPAA, HITECH and Gramm-Leach-Bliley Act) and the implementation of EHR and EMR requirements of the Affordable Care Act (ACA) require healthcare and medical practices organizations to utilize electronic records and data that is secure, and ensure methods are in place to report/recover any lost or stolen information. End-user/Organization misuse in administering and hardware fragmentation across laptops, tablets and smartphones, use of unsecured networks present a growing risk for data loss.

Frequent modification in healthcare regulations makes it a challenge for teams to provide adequate test data for agile/simultaneous releases. Inefficient test planning and coverage can result in data breaches forcing organizations to get Cyber Liability Coverage. This makes Test Data Management all the more relevant. There are only two types of Healthcare organizations right now: those that know they've been breached and those that don't know they've been breached - according to a study conducted by Ponemon Institute.

Test Data Management Strategy

With ever increasing complexities and scale of IT applications, quality and reliability of software applications is becoming critical. Test Data Management Strategy plays a very significant role in ensuring that the enterprise applications meet these standards. While delivery of these standards are becoming a real challenge for enterprises, testing teams are expected to follow precise testing methods, while ensuring a high accuracy of test data.

Build a data inventory, replication of the production-like situations, both functionally and technically is also the responsibility of the testing team. A well-defined Test Data Management Strategy can bring down data inefficiencies resulting in availability of secure test data consistently from distributed and heterogeneous data sources.

An Effective TDM Implementation

TDM works by extracting 'real' data from the production environment, applying filters and masking it, so it can be used in the test environment. TDM techniques should address creation of accurate test data where production data is insufficient or unavailable. A structured testing process ensures data to be managed by:

Health Insurer Anthem is Hacked – Exposing millions of patients' data.

The second largest health insurer in the country suffered a breach that may have exposed data on as many as 80 million current and former customers, including names, Social Security numbers, birth dates, addresses and income data³.

³ Health Insurer Anthem Is Hacked, Exposing Millions of Patients' Data:
<https://www.wired.com/2015/02/breach-health-insurer-exposes-sensitive-data-millions-patients/>

- **Extracting** - By taking a sub-set of data from live production data.
- **Masking** - It removes sensitive data contained in certain health records or data fields (e.g. SSN, PII).
- **Synthetic data** - It generates 'substitute data' to re-populate certain cells, adds new fields to create test data sets.
- **Gold copy data** - Must contain a standard set of data with which to repeatedly test, and must contain the data needed to satisfy every possible test.

Organizations have data governance teams to review and enforce mitigations to any instances of production data usage in the non-production environment. The team ensures risks are mitigated through data manufacturing, access control, and data masking as applicable. Identifying a right TDM tool and building an appropriate TDM automation strategy brings down both risks and environmental costs.

Challenges in Test Data Management

- **Huge effort spent on TDM** - Significant amount of effort and time spent in test data identification, extraction and conditioning, consume large effort in testing life cycle.
- **Regulatory and compliances** - Implementing Data compliance standards (HIPAA, HITECH and Gramm-Leach-Bliley Act) can be cumbersome.
- **Absence of traceability** - Lack of traceability between test data to test cases to business requirements leading to issues on the test data coverage.
- **Distributed data source** - Test data identification and extraction from multiple sources and environments.
- **Using production data** - Protecting production and test data by right masking and sub-setting techniques.
- **Data validity, consistency and integrity** - Ensuring test data is relevant, refreshed, secure & precise.

*Value of a healthcare data
Stolen health credentials can go for \$10 each, about 10 or 20 times the value of a U.S. credit card number in the underground exchanges⁴.*

Business Benefits of Test Data Management

An effective Test Data Management strategy can control the quality and right quantity of test to:

- Increase the testing speed by up to 25%, cut costs by 10%.
- Provide realistic test data for better & repeatable test data quality and reduce dependency on production data.
- Reduce overall testing time; faster data refresh.
- Lower hardware and infrastructure costs by creating Subset (create smaller copies of production for test purposes); create flexible test environments.
- Ensure optimum test coverage.
- Secure and compliant test data.

⁴ Your medical record is worth more to hackers than your credit card:

<https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924>

About Trigent

Trigent is a CMM Level-4 technology solutions company with its US office at Southborough, MA, and India office at Bangalore. Trigent provides comprehensive solutions for business problems via outsourced software product and applications design, development and quality assurance. Trigent serves customers like Independent Software Vendors (ISVs), enterprises and SMBs in the High Tech, Healthcare, Education, Ecommerce and Manufacturing areas. Trigent's solutions help clients overcome budget, schedule and resource constraints.

To learn more about Trigent visit www.trigent.com

Our Headquarters

Trigent Software Inc.
2 Willow Street, Suite #201
Southborough, MA 01745
+1 (877) 387-4436
sales@trigent.com

Other Location

Trigent Software Ltd.
Khanija Bhavan, 1st Floor
#49, West Wing, Race Course Road
Bangalore - 560001, India
+91 (80) 2226-3000



Microsoft Partner

Gold Application Development
Gold Collaboration and Content

