Cost of a Breach:

A Business Case for Proactive Privacy Analytics

Being a leader in patient privacy isn't just responsible from a compliance perspective - it's simply good business sense in a world where privacy-aware institutions are awarded consumer loyalty.

Annual breach costs to your institution can easily reach millions of dollars in damages, even when only a small number of patients and malicious actors are involved. With 90% of hospitals having reported a breach in the past two years, and most health systems reporting an increasing number of inappropriate accesses, the business case for Protenus is clear. From a financial risk perspective, *the Protenus platform would pay for itself if your organization avoids a single breach penalty or lawsuit due to its deployment.*

Average cost of a single data breach (all industries):

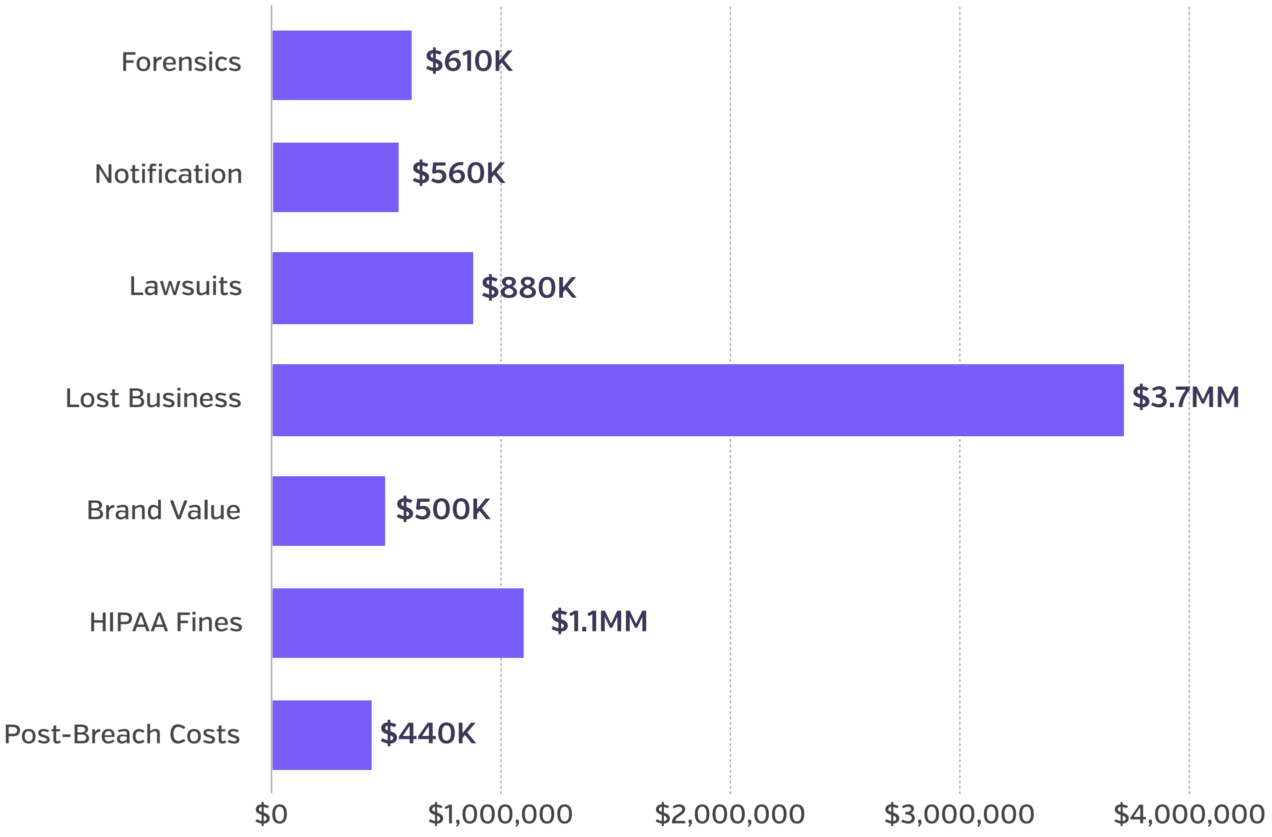
$4 Million

Today's patient data security and privacy solutions are outdated, costly, and labor-intensive, and if they are executed incorrectly, they can result in huge fines, litigation, and revenue loss. Breaches in the healthcare industry total an exorbitant $6.2 billion annually, with the average cost of a single data breach across all industries now $4 million.[1] Threats to patient data inside the EHR can come from compromised access credentials, theft, phishing attacks, or employees abusing their access. Troublingly, it takes an average of more than 200 days to detect an insider threat, if it is detected at all.[2] In that time, your patients and institution remain terrifyingly vulnerable, and the potential danger represented by this threat increases significantly.

[1] Sixth Annual Benchmark Study on Privacy & Security in Healthcare Data, Ponemon Institute

[2] FireEye: https://www2.fireeye.com/WEB-2015RPTM-Trends.html, 2015

Seven Potential Costs of a Healthcare Data Breach



Average Cost by Category for Healthcare Data Breaches

Breach costs by category vary greatly, depending on the size and nature of the breach. For smaller breaches, the primary sources of damage are lost revenue, reputation, and lawsuits. As breaches become larger, the significant costs of notifications and remediation become quite large as well.

The seven cost categories noted above are detailed to provide further insight on how advanced privacy patient monitoring can help your institution save millions.

Forensics

In the wake of a breach, either additional compliance personnel or external auditors are brought in to search through millions of access logs to determine what information was breached and who was involved. Due to the vast amount of information that auditors have to request and piece together, this process can require months of tedious work.

Ponemon averages forensics costs at $610,000

Detecting breaches the moment they occur, and with a context-rich solution, significantly reduces the scope of these investigations, as actors are often stopped from doing much more damage, and most of the information necessary is already at hospitals' fingertips. While simple "snooping" events tend to have lower forensics costs, this category becomes increasingly costly with complex insider threats.

Notification

For breaches involving greater than 500 people, hospitals are required by law to release the information to the media. These plans may involve establishing a toll-free number to take any questions about the breach, assisting with monitoring credit scores for the affected patients, and other support services.

When a large breach occurs, notification is required by HIPAA's Breach Notification Rule, 45 CFR §§ 164.400-414. However, if a persistent internal threat is detected proactively, it is often possible to stop it before it reaches a threshold necessary for reporting. Using advanced forensic capabilities to precisely determine what damage was done, rather than preemptively notify a large number of patients without knowing which ones were specifically affected, is a far preferable situation in the wake of a breach.

Ponemon averages notification costs at $650,000

Lawsuits

Health data breach lawsuits, from class action to single-patient, widely vary in cost. However, it is often small-scale breaches (of even a single record) that cause the most harm, due to their personal and visceral nature. Ponemon puts the average cost of a legal settlement after a breach in the U.S. at

$880,000, and healthcare breaches tend to be even more costly. Below are some examples.

- $865,500 settlement against UCLA after two celebrity patients alleged hospital employees reviewed their medical records without authorization
- $1.4 million settlement against a Walgreens pharmacist that snooped in husband's ex-girlfriend's medical record
- $412 million class-action lawsuit against a Scarborough hospital on behalf of thousands of patients whose personal information was leaked by two former employees
- $7.5 million for a class-action lawsuit against St. Joseph Health System for PHI made searchable on the Internet

Class action lawsuits generally cost $1000 per affected individual, so while single-patient breaches can cost millions, larger breaches can cause astronomical damage.[3]

Proactively identifying threats and notifying patients is always preferable to patients finding out about inappropriate accesses long after the event. By taking a proactive and transparent approach, hospitals find that the risks of "bad blood" and lawsuits are significantly reduced. As with all elements of compliance, by staying ahead of problems, costs and damage can be significantly reduced.

Lost Revenue

$113 million in lost revenue per data breach

A 'Global State of of Security' survey from PwC reveals that 21 percent of patients withhold information from physicians because of fear of a privacy breach, while 54 percent of respondents say they would switch providers as a result of a data breach. Healthcare providers could potentially lose $305 billion in patient revenue over the next five years due to the impact of

[3] http://www.hipaajournal.com/calculating-the-cost-of-a-hipaa-data-breach-6534/

cybersecurity attacks, according to a report from Accenture.[4] The same report notes that the average hospital will lose $113 million per data breach in lost revenue over the following five years, based on the average lifetime value of a patient and the loss of patient business that occurs post-breach. The Ponemon Institute estimates approximately $3.7 million per data breach, the more conservative estimate that we include in our graph above, but these likely understate the long-term revenue damage to an institution.

Privacy breaches aren't just about the direct costs - the indirect costs of losing patient trust mean that you can lose the trust that brings patients back for your services. By maintaining that trust and goodwill, patient churn is reduced and you can recover rapidly (or suffer very little impact) from lost patient revenue.

Brand Value

The most damaging types of breaches are those that lose customer data, and they can have wide-reaching effects.[5] While figures vary widely for "loss of brand," and can be highly subjective, the median loss of brand figure post-data breach was reported at $500,000, with some estimates reaching $50 million.[6] Depending on your institution's scope, reputation, and coverage area, appropriately valuing this risk is a highly-personalized decision for senior leadership.

$500,000 median lost brand value following a breach

A patient privacy program helps preserve an institution's reputation, and create a culture of trust that serves as a competitive advantage in an increasingly-undifferentiated marketplace. A precise estimate of damage to your brand is difficult to capture, but any hospital leader knows that it is far from a theoretical concern.

[4] https://www.accenture.com/t20150723T115443__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_19/Accenture-Provider-Cyber-Security-The-$300-Billion-Attack.pdf

[5] https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

[6] https://www.sans.org/reading-room/whitepapers/analyst/cleaning-breach-post-breach-impact-cost-compendium-36517

Fines

Since 2008, there have been 39 HIPAA privacy and security rule investigations by the OCR that have led to monetary payments, either via settlement agreements or legal actions, many of which reach millions of dollars. The average fine amount is approximately $1.1 million, but this average is trending upward in the past few years. These fines are only expected to increase in frequency and severity, as OCR rolls out their Phase 2 audit program, and comes under increased pressure to protect patient privacy.[7] In addition, individual states often have the ability the levy separate penalties that augment federal statutes.

Largest fine thus far: $5.55 million

Annual maximum for OCR fines: $1.5 million per violation category

While OCR settlement decisions are somewhat arcane, one clear pattern emerges throughout - individuals who have a strong plan and go “above and beyond” are rewarded.

Post Breach Costs

Cleaning up after a breach can vary widely and can include purchasing new technologies, new staff, putting in place onerous processes, complying with regulations, and more.

Hospitals must then mitigate public defamation by setting up remediation plans for patients whose data is at risk. Although hospitals are not required to offer a remediation plan, they will often have one to help defer the chance of a lawsuit or assist in the settlement of a formal OCR action. Even a basic piece of auditing technology and two FTEs on your privacy team can quickly add up to hundreds of thousands of dollars annually.

With an industry-leading privacy analytics platform already in place, and one that uses advanced analytics to avoid the need for additional staff and managed services, your hospital can help keep post-breach costs to a minimum while still maintaining a superlative level of protection for your institution.

[7] http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html