accenture

Strategy | Consulting | Digital | Technology | Operations

INSIGHT DRIVEN HEALTH

Digital Health

# The $300 Billion Attack:

## The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction

High performance. Delivered.

As cyber attackers strike clinical and financial systems, healthcare providers that do not protect and defend their patients' data could lose customers and billions in patient revenue.

**Healthcare providers that do not make cyber security a strategic priority will put $305 billion of cumulative lifetime patient revenue at risk over the next five years, Accenture analysis shows.**

The significant increase in adoption and use of electronic medical records (EMRs) and other healthcare technology has created a wealth of electronic information that includes patient data such as dates of birth, home addresses, social security records, insurance details and medical data.

This treasure trove of information is increasingly being targeted by cyber attackers. In 2014, nearly 1.6 million people had their medical information stolen from healthcare providers, according to the U.S. Department of Health and Human Services Office for Civil Rights.* Accenture analysis predicts more than 25 million people—or approximately one in 13 patients—will have their medical and/or personal information stolen from their healthcare provider's digitized records between 2015 and 2019 (Figure 1). In many cases, the patient's response could be to walk away from the healthcare provider that failed to protect his/her data.

### Victims suffer personal financial loss

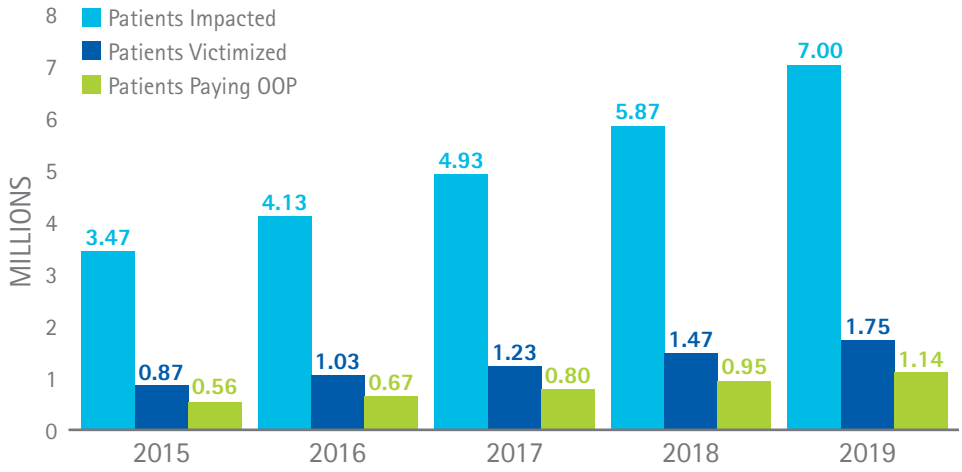
What most healthcare providers don't recognize is that as a result of cyber attacks on medical information, many patients will suffer personal financial loss. In contrast to credit card identity theft, where the card provider generally has a legal responsibility for account holders' losses above $50, victims of medical identity theft often have no automatic right to recover their losses.

According to the Ponemon Institute, these financial losses may take several forms. Not fully understanding their medical bills, some victims have unwittingly paid bills run up by others. Some have had to reimburse their insurers for healthcare services obtained fraudulently. Many have incurred substantial legal costs as they have sought to unravel the cyber crimes perpetuated against them. In fact, 65 percent of victims of medical identity theft pay out-of-pocket (OOP) costs at an average of $13,500 per victim.

Accenture projects that 25 percent of patients impacted by healthcare provider data breaches between 2015 and 2019—more than 6 million people—will subsequently become victims of medical identity theft. Sixteen percent of impacted patients—more than 4 million people—will be victimized and pay out-of-pocket costs totaling almost $56 billion over the next 5 years.

**Figure 1:** 2015-2019: Medical and personal information theft due to healthcare provider data breaches will impact 1 in 13 patients

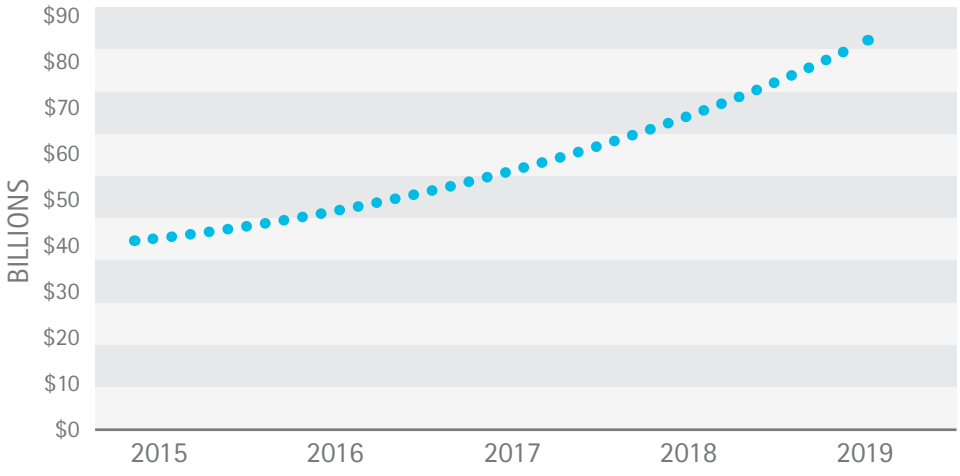
~25 million patients will have their medical information stolen.
~6 million patients will become medical identity theft victims.
~4 million patients will pay out-of-pocket costs related to medical identity theft




*Source: Accenture analysis*

**Figure 2:** 2015-2019: Healthcare providers could lose $305 billion in cumulative lifetime revenue from patients impacted by medical identity theft

Cumulative lifetime patient revenue loss 2015 to 2019 ~$305 billion




*Sources: Accenture analysis, HHS Office for Civil Rights, Ponemon Institute*

## Healthcare providers take the blame – and suffer the consequences

Healthcare providers will pay a heavy price for cyber security complacency. Almost half of patients said they would find a different provider if they were informed that their medical records were stolen. Taking into account the estimated lifetime economic value of a patient, Accenture analysis shows that healthcare providers are at risk of losing $305 billion in cumulative lifetime patient revenue over the next five years due to patients switching providers because of medical identity theft (Figure 2). Applying this methodology to recent healthcare provider data breaches, Accenture estimates that each provider organization lost an average of $113 million of lifetime patient revenue for every data breach it suffered in 2014.

## Time for active defense

To prevent revenue loss on this scale, healthcare providers must prioritize improvements of their cyber security in order to thwart attacks that aim to steal patient data from clinical and financial systems. Moving to active defense strategies can improve cyber security effectiveness by an average of 53 percent over two years, Accenture research shows. This is increasingly important as recent events have shown that a provider's cyber security insurance may not be able to be claimed without adequate security standards and controls in place.

Active defense requires a risk-based approach to cyber security management, using analytics to detect events and threats, as well as enabling a far swifter response to incidents. In this era of digital health, ehealth and health care consumerism, this shift must be a priority for C-level healthcare executives, rather than the sole responsibility of the information or technology function, with strategic planning to identify and then close potential vulnerabilities.

**Figure 3:** 5 Actions Healthcare Providers Can Take to Develop Effective Cyber Security Measures

How to handle vulnerabilities and mount an active defense to **meet** and **deflect attacker advances**

| Assess security capability, identify opportunities | Manage complexity and integrate the enterprise | Become agile | Accelerate toward security intelligence | Develop end-to-end delivery and sourcing |
|---|---|---|---|---|
| Determine where the organization currently stands and the level of resources required to support meaningful transformation | Evolve the security program vision: establish an end-to-end enterprise security program and integrate it with existing enterprise architecture processes to reduce complexity levels and produce outcomes valued by the business | Embrace the cloud and other emerging technologies to boost IT agility and reach customers faster, capitalize on efficiency and cost benefits and do so within risk tolerances | Adapt to handle new threats to the enterprise by developing threat-centered operations by developing a deep understanding of adversaries, their goals and techniques | Plan a delivery and operational strategy for each of the security services they offer to make a clear-eyed assessment of internal competencies for designing, building and deploying elements of a cyber-security program |

*Source: Accenture*

Healthcare providers that successfully make this leap will limit the damage cyber attackers can cause. Active defensive measures can safeguard future patient revenue that will otherwise be lost to competitors and also safeguard consumers who have entrusted providers with their medical and financial information.

## Methodology

Accenture used historical security breach data from the U.S. Department of Health and Human Services Office for Civil Rights to project the number of patients impacted by healthcare provider data breaches 2015-2019. Based on medical identity theft information by the Ponemon Institute, Accenture calculated the impacted patients that would become victims of medical identity theft and quantified the patient revenue that would be put at risk.

## For more information:

**Brian Kalis**
brian.p.kalis@accenture.com

**Jennifer Combs**
jennifer.l.combs@accenture.com

**Janessa Nickell**
janessa.nickell@accenture.com

## Glossary of terms

**Lifetime patient revenue:** Total economic value or total patient revenue over the lifetime of an individual patient.

**Cumulative lifetime patient revenue:** Total lifetime patient revenue for a group of patients.

**Medical information theft:** The crime of stealing patient personal information (including clinical and/or financial information).

**Medical identity theft:** The crime of fraudulently using an individual's name and personal identity to receive medical services, prescription drugs and/or goods, including attempts to commit fraudulent billing.

**Impacted patients:** Patients who have their personal information stolen in a data breach (as reported to the U.S. Department of Health and Human Services Office for Civil Rights for breaches impacting 500 or more people).

**Victimized patients or medical identity theft victims:** Patients who have their personal information stolen in a data breach and whose information is subsequently used in a fraudulent manner.

*Security breaches impacting more than 500 people must be reported by healthcare organizations to the U.S. Department of Health and Human Services Office for Civil Rights.

## About Accenture Insight Driven Health

Insight driven health is the foundation of more effective, efficient and affordable healthcare. That's why the world's leading healthcare providers and health plans choose Accenture for a wide range of insight driven health services that help them use knowledge in new ways— from the back office to the doctor's office. Our committed professionals combine real-world experience, business and clinical insights and innovative technologies to deliver the power of insight driven health.
For more information, visit: www.accenture.com/insightdrivenhealth.

## About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 336,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.



12460224