accentureconsulting

DIGITAL TRUST

Are You One Breach Away From Losing a Healthcare Consumer?

Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

United States consumers trust healthcare organizations to protect their digital data—and they may be unforgiving of failure

According to an Accenture survey, healthcare consumers believe that payers and providers are taking measures to protect patients' digital healthcare data, yet 26 percent of consumers have experienced a data breach. In response, 25 percent of consumers who experienced a breach changed providers, 21 percent changed payers and 19 percent got legal counsel. Interestingly, despite the myriad breaches occurring, consumers are more confident in their providers and payers than in government and health technology companies.

To better understand consumer attitudes toward healthcare data, digital trust, roles and responsibilities, data sharing and breaches, Accenture conducted a survey across seven countries. This report focuses on results from consumers in the United States and on healthcare-specific cybersecurity and digital trust.

By examining digital trust and the impact of breaches, healthcare organizations can better understand risks, the importance of building resilience and security capability and the need to respond proactively, should a breach occur.

Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

DIGITAL HEALTHCARE DATA

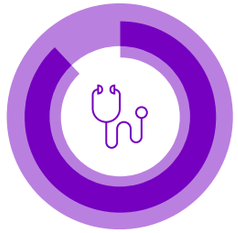
Personal health information that is stored electronically, such as in electronic health records maintained by a person's doctor or healthcare provider, wearable health devices, mobile apps or health insurance records.

DIGITAL TRUST

The confidence placed in an organization to collect, store and use the digital information of others in a manner that benefits and protects those to whom the information pertains.

Healthcare consumers don't trust everyone with their data

A significant majority of consumers (88 percent) trust their physicians or other healthcare providers to keep digital healthcare data secure. In fact, 36 percent have "a great deal" of trust in these entities. Nearly the same percentage of people trust their pharmacy (85 percent), the hospitals they visit (84 percent), their health insurance company (82 percent) and diagnostic labs (82 percent). Far fewer trust the tech companies (57 percent) that develop the wearables and health apps that they use, or the government (56 percent). (Figure 1)



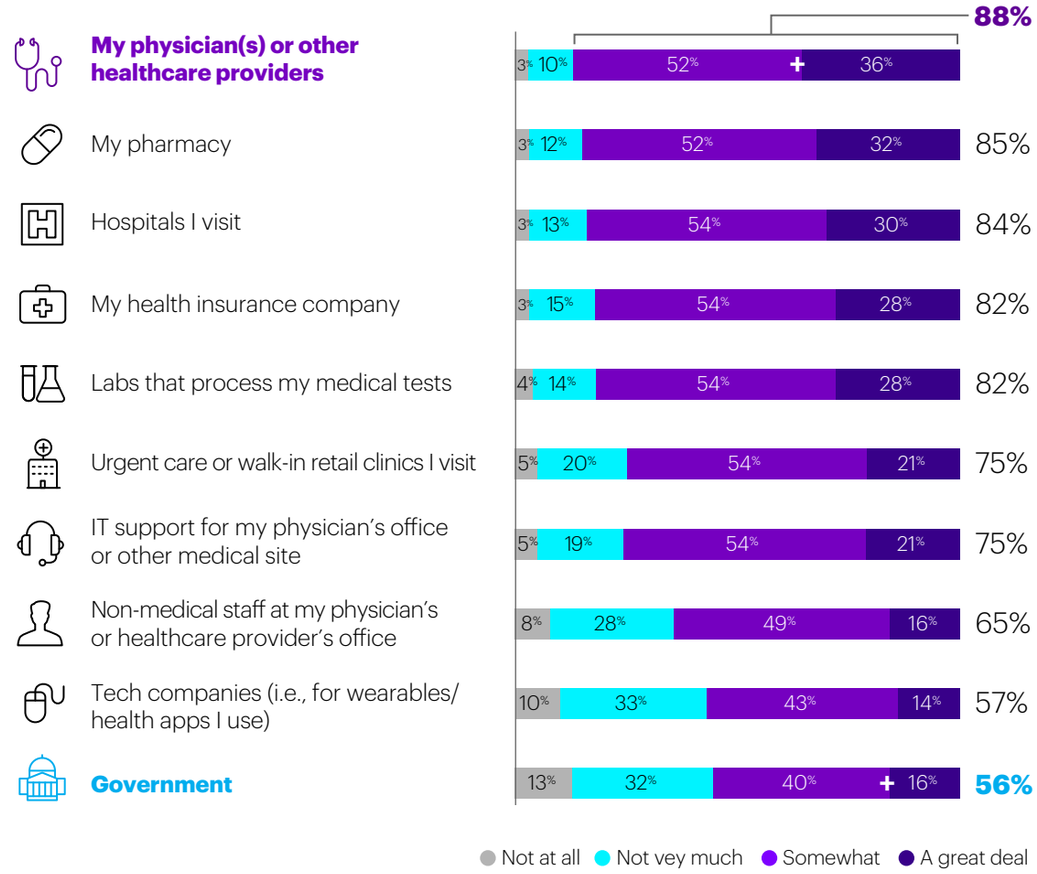
MOST TRUSTED

88% **My physician(s) or other healthcare providers**

LEAST TRUSTED

56% **Government**

FIGURE 1: Healthcare consumers have varying degrees of trust in healthcare organizations.

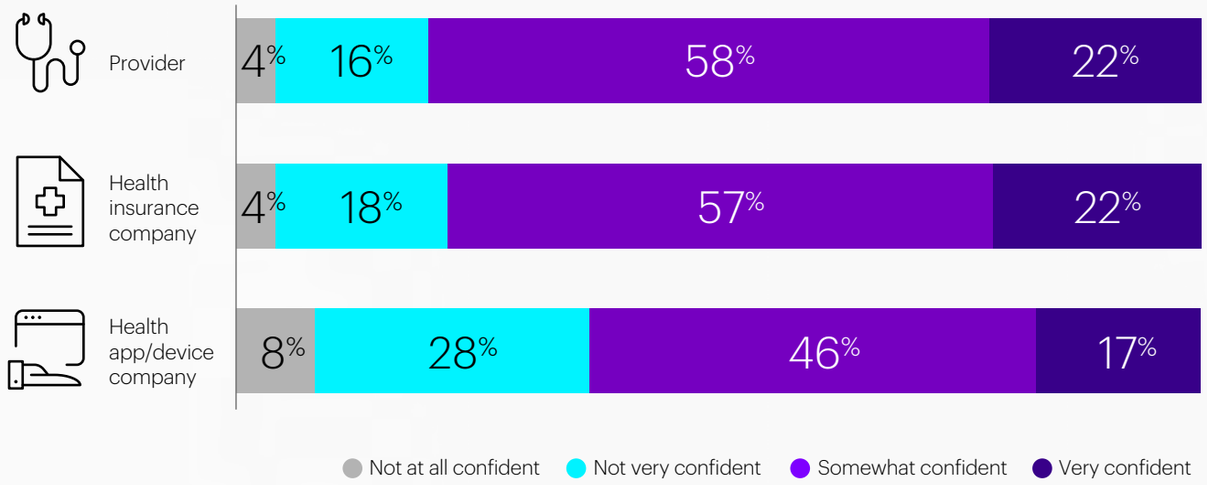


Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

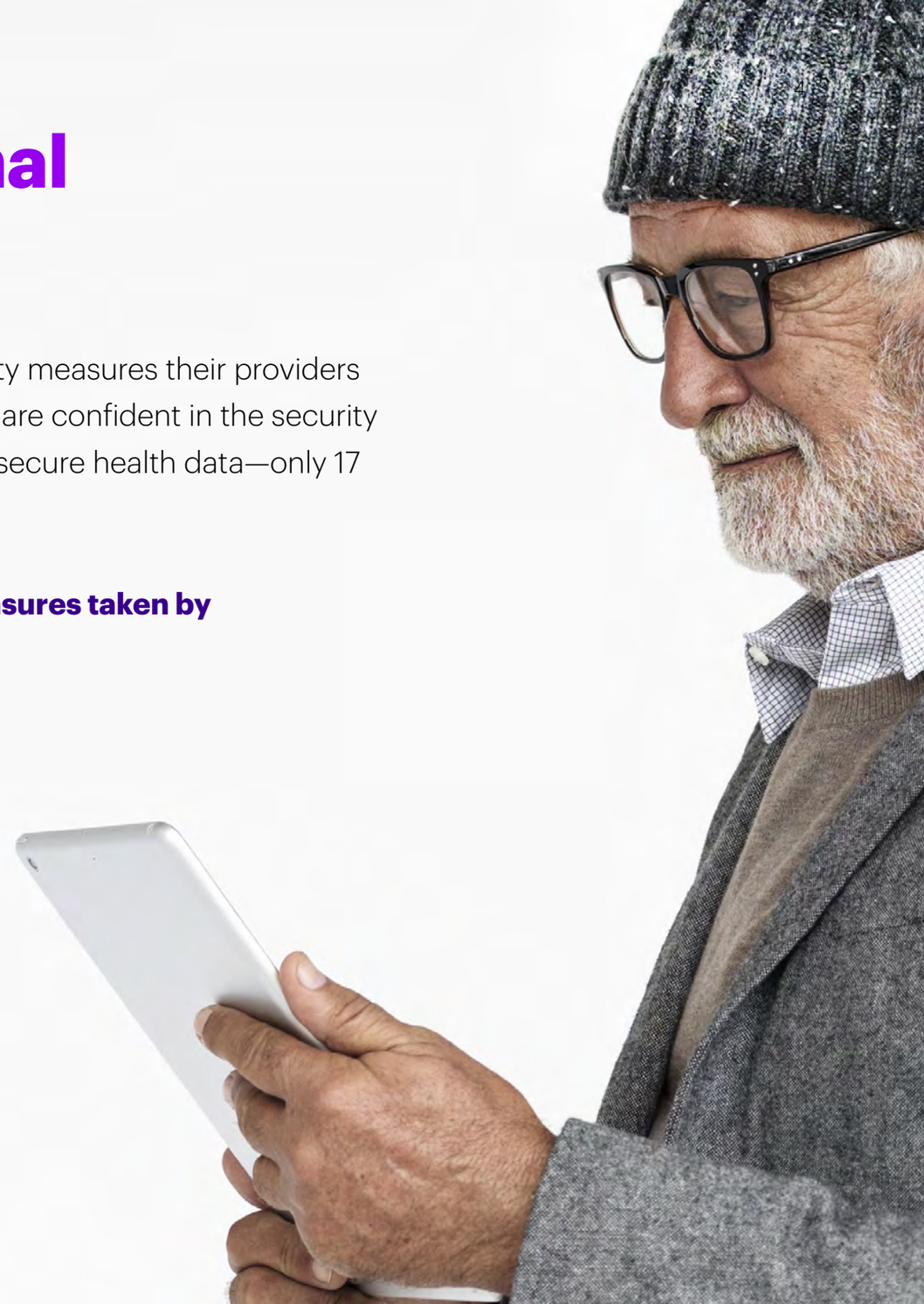
Confidence lies in more traditional healthcare relationships

A majority of US consumers have at least some confidence in the digital data security measures their providers and insurers are taking, 80 percent and 79 percent, respectively. Fewer (63 percent) are confident in the security measures that health app and device companies have taken to protect privacy and secure health data—only 17 percent are very confident in these companies. (Figure 2)

FIGURE 2. Healthcare consumers have greater confidence in the security measures taken by healthcare providers and insurers than in those by app/device companies.



Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust



Despite consumers having trust in healthcare organizations, healthcare data is being stolen

One out of four US healthcare consumers (26 percent) has experienced a breach of their digital healthcare data, which may include their Social Security number, contact information, electronic medical record or health insurance ID. Half of those people were victims of medical identity theft. Of those, most often the stolen identity was used to purchase items (37 percent). Stolen IDs were also used for other fraudulent activities that include billing for care, receiving care and filling prescriptions (Figure 3). Among those who experienced identity theft, most consumers report the incident cost them an estimated $2,528, on average, per incident.

FIGURE 3. Victims of medical identity theft report stolen IDs were used for fraudulent activities.

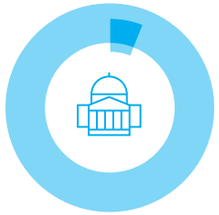
Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

Breaches may not happen where consumers expect them

Among those consumers who experienced a breach, one-third (36 percent) said it occurred in a hospital—the third most trusted entity to keep data secure—while one-fifth (22 percent) said the breach happened at an urgent care clinic, pharmacy (22 percent), physician's office (21 percent) or health insurance company that was holding their data (21 percent). Interestingly, the lowest percentage of breaches (6 percent) occurred at a government entity—which is the entity that consumers trust the least to keep digital health data secure. (Figure 4)

HIGHEST PERCENTAGE OF BREACHES OCCURRED

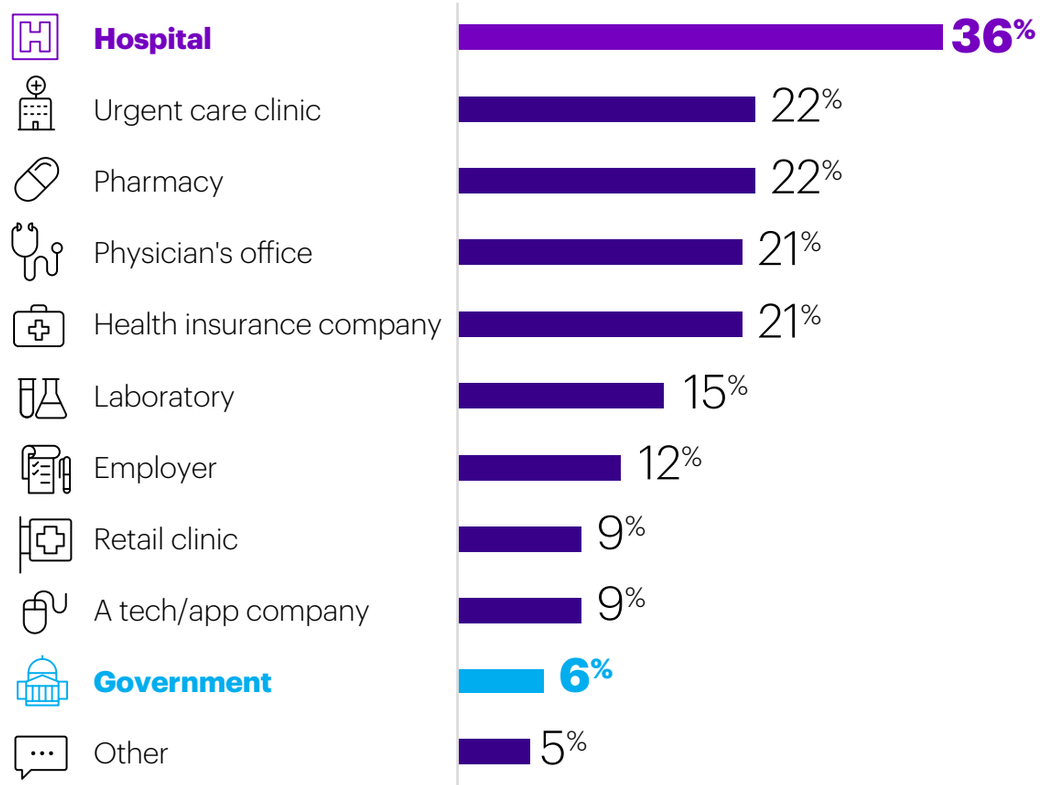
36% **Hospital**



LOWEST PERCENTAGE OF BREACHES OCCURRED

6% **Government**

FIGURE 4. Digital healthcare data breaches are occurring across a variety of locations.



Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

Finding the breach

Half of consumers who experienced a breach found out about it themselves. Just fewer than half (45 percent) were proactively notified and about one-third (36 percent) learned about the breach passively. (Figure 5)

What are healthcare data thieves taking?

Among those consumers who experienced a breach, nearly one-third (31 percent) had their Social Security number stolen. The same percentage had contact information or electronic medical records compromised. Biometric identifiers were the data least frequently compromised in a breach (10 percent).

Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

FIGURE 5. Most often, healthcare consumers noticed errors themselves.

50% **ERROR NOTICED BY RESPONDENT**

Noticed error in health records, credit card statement, credit report, Explanation of Benefits

45% **WAS NOTIFIED PROACTIVELY BY ENTITY/GOVERNMENT**

Received a notice from provider; government entity informed me

36% **LEARNED ABOUT IT PASSIVELY**

Heard about it in the news; received collection letter for services not received

8% **SOME OTHER WAY**

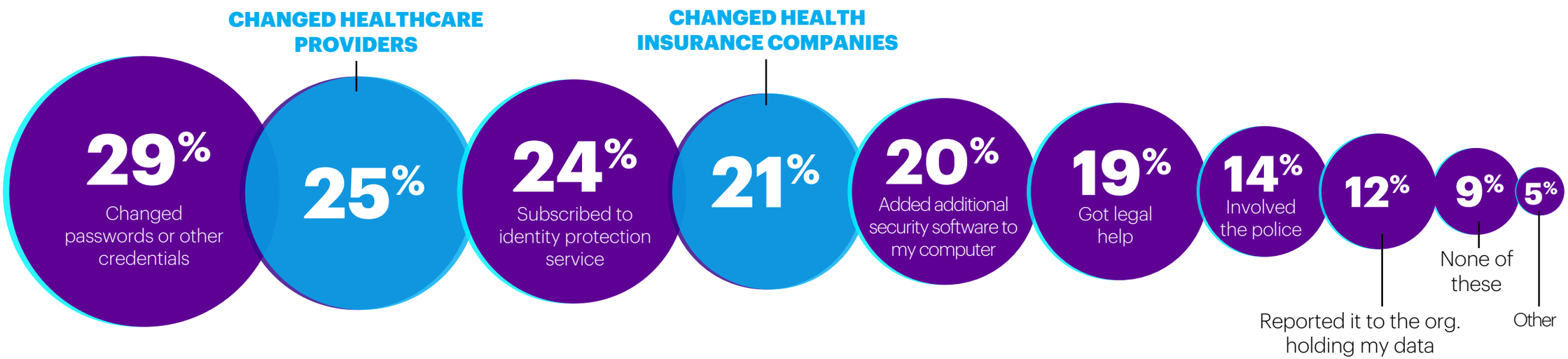
Consumers take action after breaches, sometimes against healthcare organizations

In response to the breach of their healthcare data, nine out of 10 (91 percent) consumers took action to protect their data. They changed passwords or other credentials (29 percent). Some (24 percent) subscribed to an identity protection service or added security software to their computer (20 percent).

Some consumers took action against their providers or insurance plans. One-quarter of those experiencing a breach changed healthcare providers (25 percent) and 21 percent changed their insurance company as a result of a breach. Others sought legal help (19 percent) or involved the police (14 percent). (Figure 6)

FIGURE 6. Consumers react to a breach in ways that go beyond changing passwords.

91% of consumers took steps in response to a breach



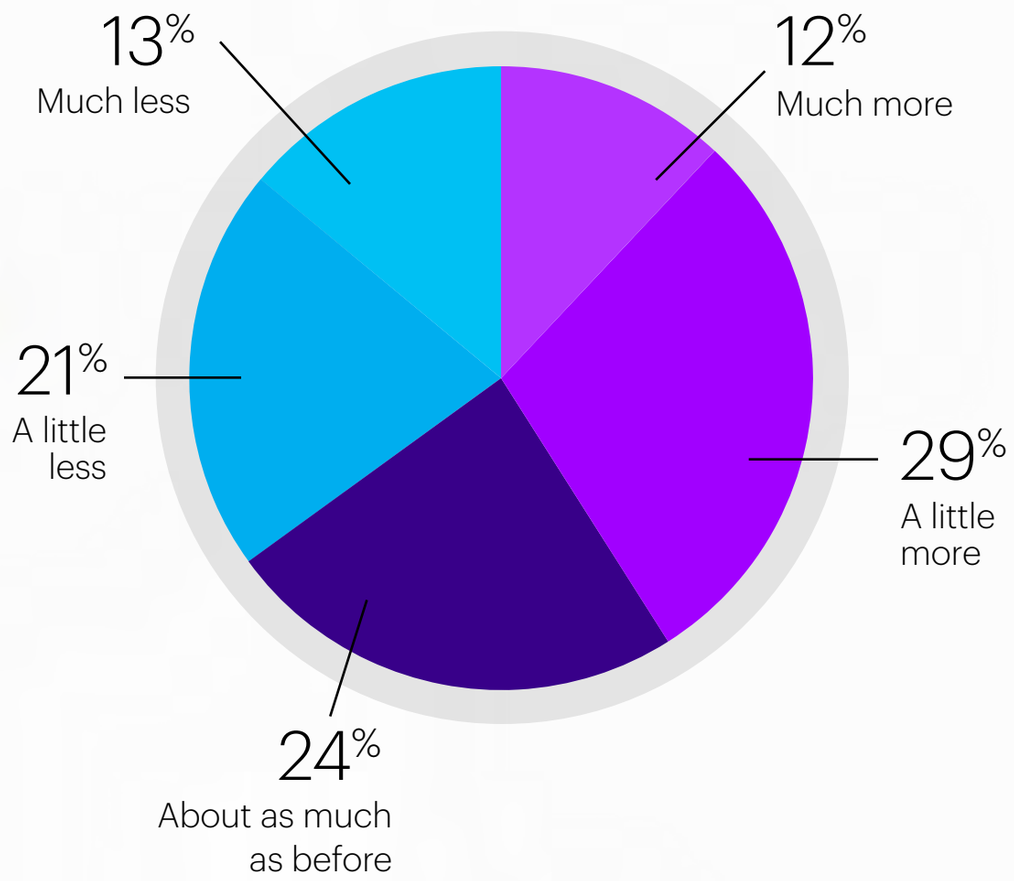
Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

Healthcare data breaches can harm digital trust

In response to the breach, nine out of 10 (91 percent) consumers reported that the company holding their data took some action. Three-quarters (76 percent) felt the breach was handled "very well" or "somewhat well."

Interestingly, following a breach, 41 percent of consumers gained trust in the organization, 24 percent reported no change in their trust and 34 percent lost trust. (Figure 7)

FIGURE 7. After a breach, consumers report how it impacted their trust in the organization.



Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

Improving cybersecurity is the first step in building digital trust

Breaches are inevitable. Healthcare organizations can try to protect against them, but moreover, they should establish digital trust early on to build a foundation that helps consumers to weather the storm of a breach. According to Accenture analysis, healthcare providers that do not make cybersecurity a strategic priority will put $305 billion of cumulative lifetime patient revenue at risk over the next five years.[1]

Now is the time for healthcare providers, health plans and other organizations to strengthen cybersecurity capabilities, improve their defenses, build resilience and better manage breaches. Most importantly, they can give consumers the confidence that their data is in trusted hands.

KEY ACTIONS TO FOCUS ON:

IMPROVE RESPONSE CAPABILITIES

In conjunction with improving detection, handle breaches quickly and efficiently, in a way that limits damage.

VALIDATE DOWNTIME PROCEDURES

Strive to reduce recovery time to minimize impact on patient care and business operations.

SHARE THREAT INFORMATION

Act on learnings and share them with others. Communicate to consumers the actions you have taken.

RE-BOOT YOUR APPROACH

Embrace an end-to-end cyber defense that recognizes a spectrum of threats, minimizes exposure, and identifies and protects high-priority assets.

MANAGE YOUR RISKS

Make targeted cybersecurity investments that will deliver measurable returns and help you build digital trust with healthcare consumers, who are increasingly security-aware.

1: Accenture; "The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction;"

Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

For more information

Kaveh Safavi

kaveh.t.safavi@accenture.com

Kip Webb

kip.webb@accenture.com

Reza Chapman

reza.j.chapman@accenture.com

Follow us on Twitter

@AccentureHealth

Accenture Health

Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

Accenture commissioned a seven-country survey of 7,580 consumers ages 18+ to assess their attitudes toward healthcare data, digital trust, roles and responsibilities, data sharing and breaches. The online survey included consumers across seven countries: Australia (1,000), Brazil (1,000), England (1,000), Norway (800), Saudi Arabia (850), Singapore (930) and the United States (2,000). The survey was conducted by Nielsen on behalf of Accenture between November 2016 and January 2017. The analysis provided comparisons by country, sector, age and use.

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 leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.