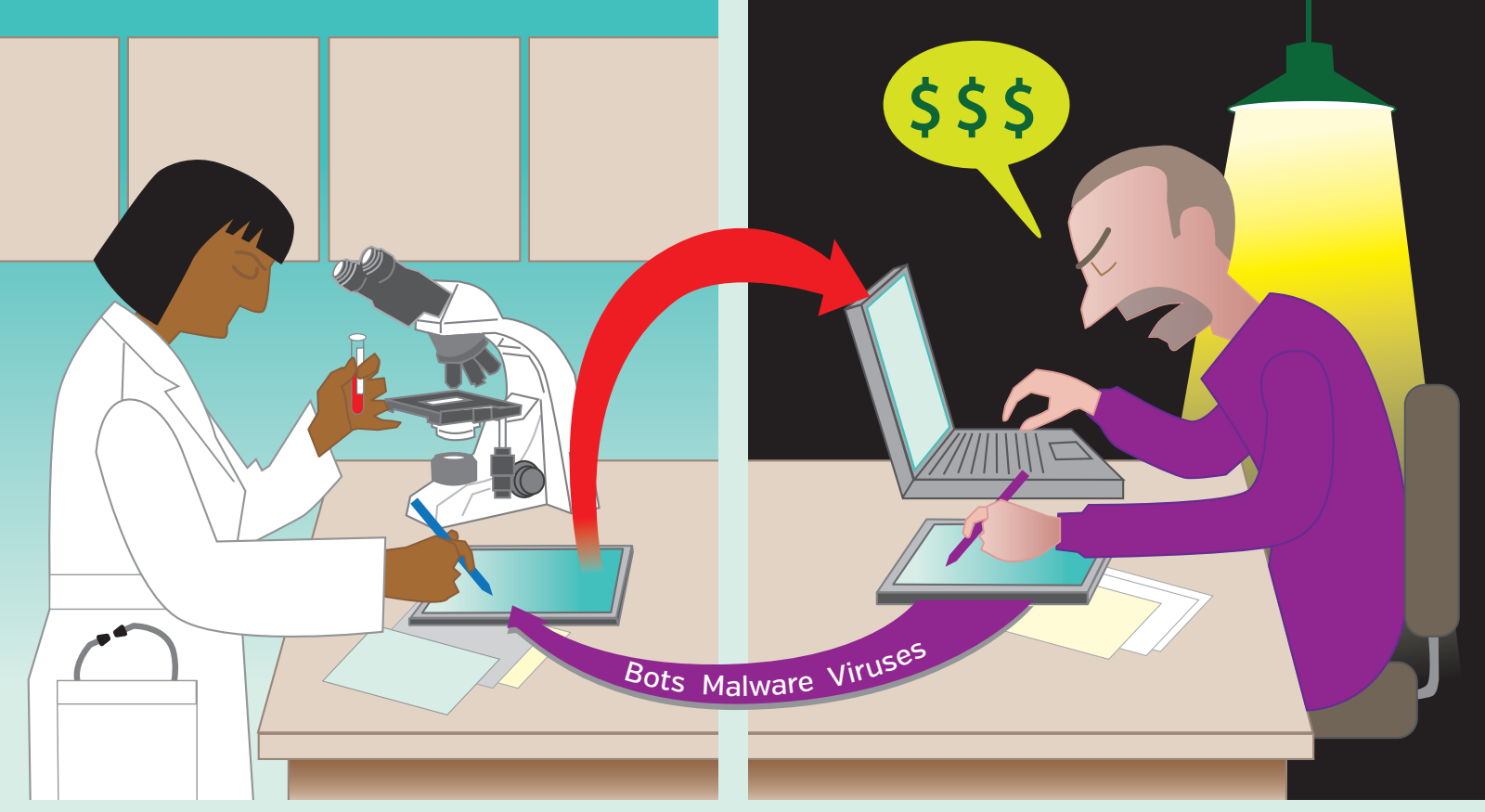


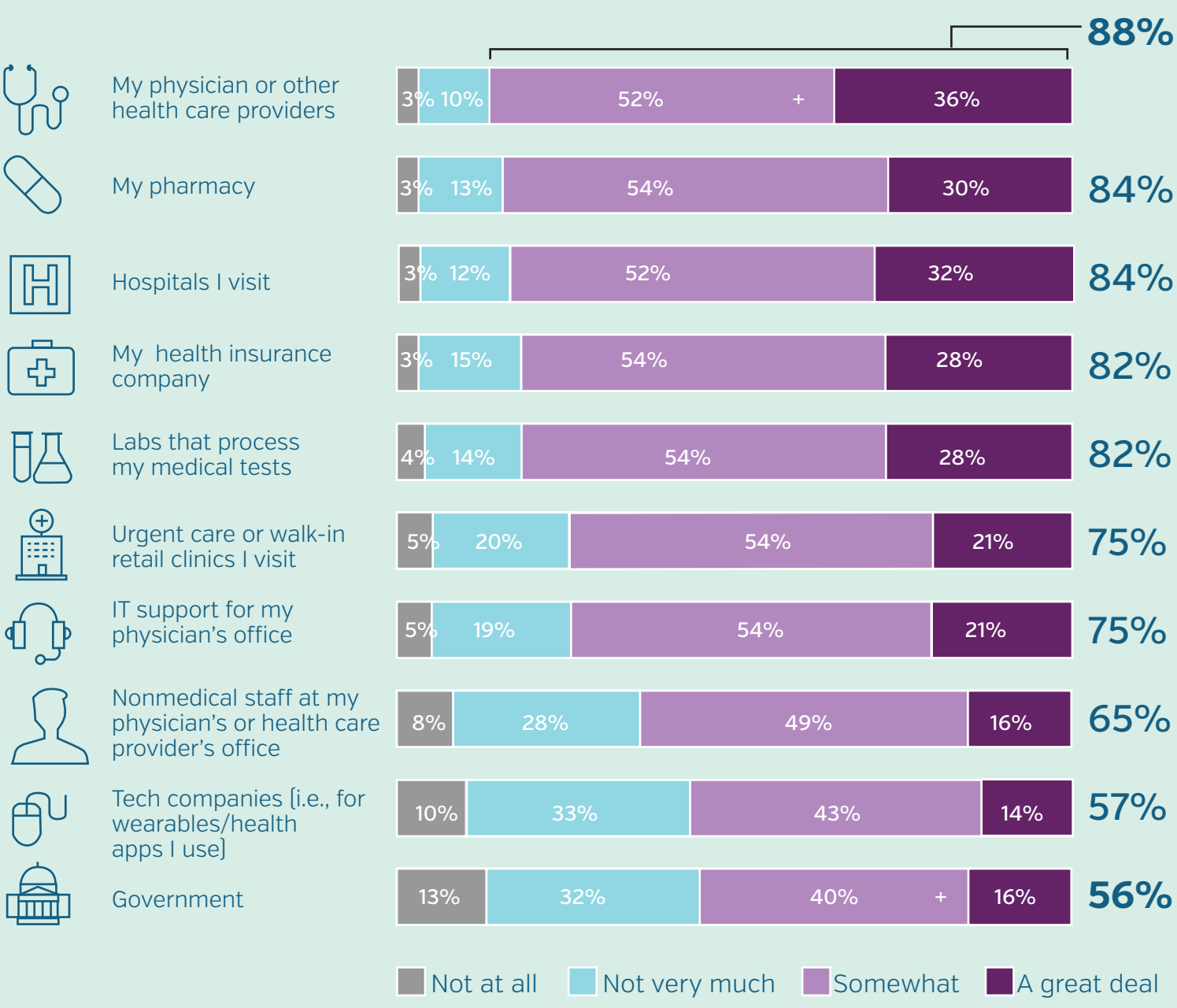
Health care data security under a microscope

Many consumers think health care organizations are protecting their personal information, according to an Accenture survey, yet 26 percent have experienced a data breach. Following such an incident, they're likely to take action, which can include changing providers.

Personal contact influences level of trust

Most consumers trust their health care providers and pharmacies to keep digital health care data secure. The government inspires less confidence.

Health care consumers have varying degrees of trust in health care organizations



Personally identifying information exposed

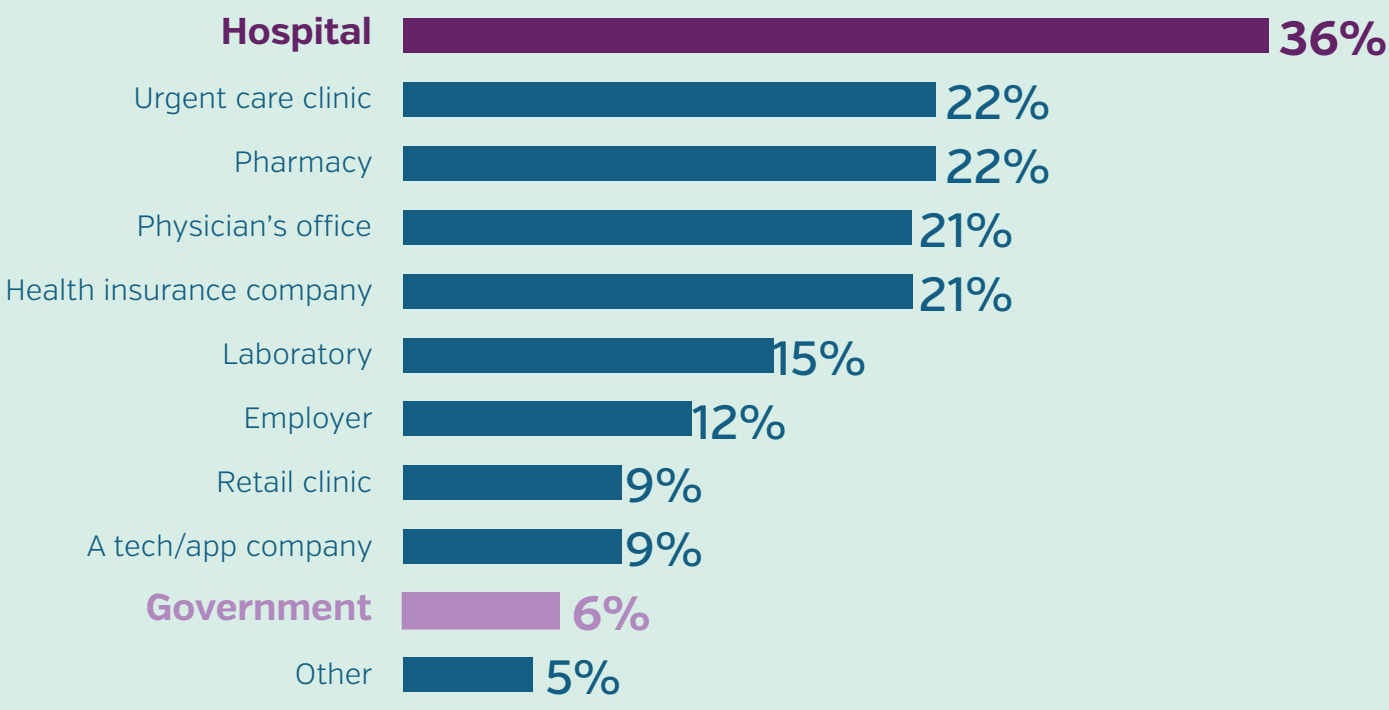
A quarter of consumers have seen their digital health care data breached, exposing Social Security numbers, contact information, electronic medical records or health insurance ID numbers. Half those people were victims of medical identity theft.

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

Checking into the hospital might not check hackers

Of consumers who had their data breached, a third said it occurred in a hospital, despite such facilities being among the most trusted to keep information safe.

Digital health care data breaches are occurring across a variety of locations

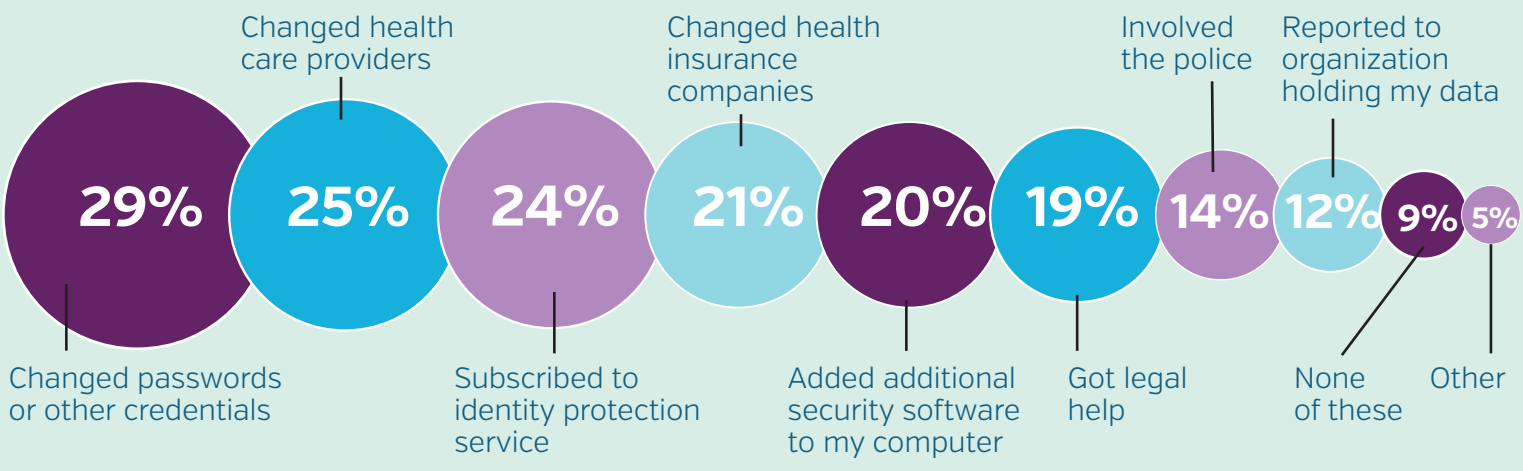


Loss of security prompts action

Most consumers who are victims of a breach take action to protect their information, such as changing passwords. Some changed companies.

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

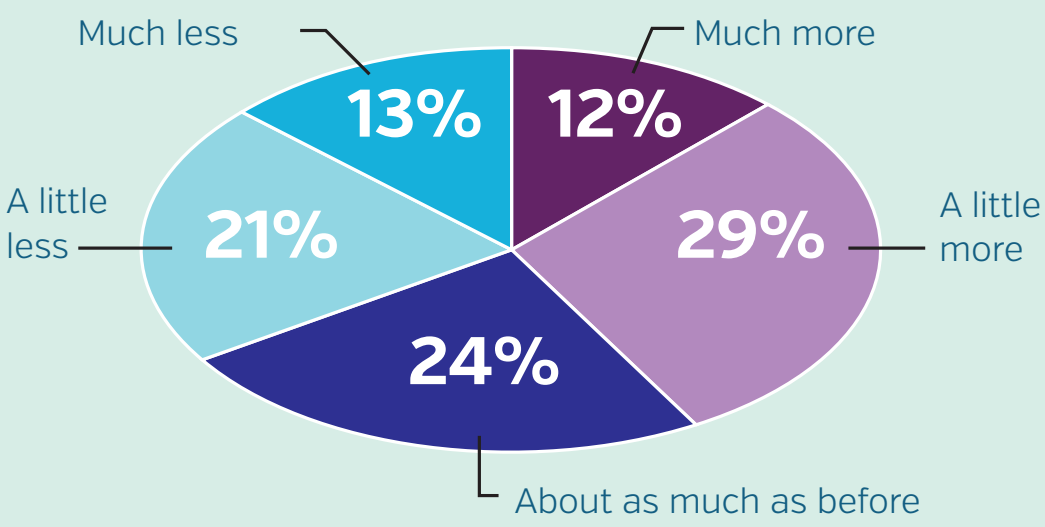
91% of consumers took steps in response to a breach



Breach's impact on trust can vary

Most consumers say that breached companies that held their data handled the aftermath of the incident well. Some came to trust such organizations more than before.

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



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