DATA SECURITY

PROTECTING CONSUMERS' DATA IN A DIGITAL WORLD

Protecting consumer data is a priority for CareFirst BlueCross BlueShield (CareFirst). Ensuring the confidentiality, integrity and availability of our systems is a necessary part of maintaining trust and delivering high-quality services to our customers and providers.

Recognizing the importance of protecting Americans' health information, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. Since then, HIPAA has become the cornerstone of privacy and data security in the healthcare industry. While a lot has changed since 1996, the regulatory framework established under HIPAA continues to ensure those entrusted with consumer data protect it.

Policymakers can do more to protect consumer data:

1 Protect Consumer Health Information, Wherever it Resides

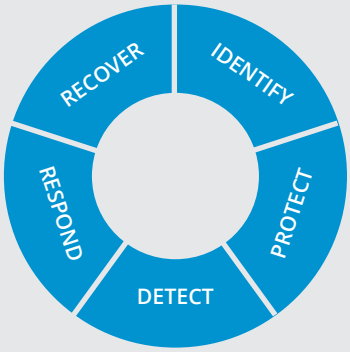
Policymakers should do more to ensure that entities collecting, using, storing or disclosing health information have reasonable safeguards to protect consumer health data. From smartwatches to fitness apps, many devices are collecting sensitive health information, but most of these platforms are not subject to the data protection requirements in HIPAA.

2 Regulatory Harmonization

Federal and state policymakers continue to enact mandates imposing new cybersecurity requirements on the private sector. Policymakers should continue to work toward aligning security requirements to support compliance. Aligning new cybersecurity requirements with existing standards, such as NIST's Cybersecurity Framework, and other established statutory and regulatory requirements like HIPAA, is vital to the success of other policy priorities like interoperability.

MORE THAN 3,600,000

members entrust CareFirst with their data.



NIST'S CYBER SECURITY FRAMEWORK

has been widely adopted in the public and private sectors and others should align with it.

95% OF BREACHES

in healthcare were financially motivated with bad actors often targeting financial data or perpetrating ransomware attacks (Verizon 2022).

3 Incident and Breach Notification

Incident and breach notification requirements can be important for sharing information with regulators to work against bad actors. In addition to federal requirements, most states have their own breach notification requirements, and different sector-specific regulators have their own requirements making compliance onerous. Policymakers should explore ways to reduce the complexity and costs associated with compliance while continuing to differentiate between reporting requirements for information sharing and reporting requirements to regulators that may result in enforcement actions.

4 Collaboration from Regulators

Federal law and policy emphasize the importance of collaboration between the government and the private sector to protect consumers and their data. As the security environment rapidly evolves, regulators should prioritize collaboration with industry, including in investigations.

5 Promote Flexibility to Account for New Technologies

As technology evolves, policymakers and regulators should embrace risk-based frameworks instead of prescriptive mandates for specific technologies or solutions.

6 Develop Programs to Build the Nation's Cyber Workforce

As the public and private sectors struggle to recruit and retain a cybersecurity workforce, policies and programs to invest in cyber education, offer hands-on training and develop the nation's cybersecurity workforce would support businesses and government and enhance the nation's cybersecurity.

686 BREACHES

were reported in 2022. Each of these cybersecurity incidents affected the protected health information of over 500 people. (HHS).

ZERO TRUST

is an increasingly popular security strategy to require additional authentication within an organization's network. CareFirst along with many others in the healthcare industry are working toward implementing Zero Trust architectures to enhance protections on consumer data.

50 NFL STADIUMS

could be filled by the 3.5 million unfilled cybersecurity jobs from 2021.

350% INCREASE

in unfilled cybersecurity jobs from 2013. (CyberVentures)

CST6084-1E (2/23)