HIPAA

Summary

Regulation: Health Insurance Portability and Accountability Act

Abbreviation: HIPAA

Governs these parties: all organizations that: receive payment for their services and transmit personal or health information for the purposes of treatment, operations, billing, or insurance coverage

Enforced by: the Department of Health and Human Services (HHS), Office for Civil Rights (OCR), the Centers for Medicare and Medicaid Services (CMS), the Federal Drug Administration (FDA), and the Federal Communications Commission (FCC)

Details

HIPAA is a series of regulatory standards that outline the lawful use and disclosure of protected health information (PHI). PHI includes private information such as past, present, or future physical or mental health or conditions, health care, past, present, or future payments for health care, and personal identifying information such as birthdates, social security numbers, and biometric information. Included in the regulations is the requirement for the security of electronically protected health information (e-PHI), which is all private data that is created, received, maintained, or transmitted in electronic form.

The rest of this document is designed to help our community understand HIPAA better by outlining the following information.

- **How it Relates to Cybersecurity**
- **How Coro Handles Compliance for You**

How it Relates to Cybersecurity

HIPAA comprises privacy, security, and breach notification rules. The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. Much of the technical safeguards described are cybersecurity guardrails, and as such require that your electronic data be monitored and protected by a security platform.

The Office of Civil Rights (OCR) offers an audit protocol that can be used as a roadmap when planning and ensuring your and your customer's data is protected.