PRESCIENT SECURITY

Handling HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) establishes federal standards that protect sensitive health information from disclosure without patient consent, enacted in 1996 by the US Department of Health and Human services.

Privacy Rule Vs. Security Rule

Where the HIPAA Privacy Rule was issued to enforce the protection of individuals' medical records and other individually identifiable health information, the Security Rule enforces the IT protocols put in place to safeguard that data.

The HIPAA Certification Process

HIPAA certification for organizations involves an independent third-party audit to certify and confirm that **seven areas** of compliance related to the physical, technical, and administrative safeguards required for HIPAA compliance have been met.

HIPAA
TESTED & ATTESTED
PRESCIENT SECURITY

Prescient Security offers HIPAA, PHIPA, and PIPEDA to help organizations protect sensitive patient data and demonstrate a commitment to privacy and health discretion at the most rigorous security standard.

Who Needs a HIPAA Audit?

A **covered entity** under HIPAA is any entity that handles, stores, or processes personally identifiable information that arises in the course of providing health care, as well as any contracted vendors who may access that data.

Examples Include:

Hospitals, Clinics, Dentists, Chiropractors, Pharmacies, Nursing Homes, and and other medical providers (all handle large amounts of PHI)

Insurance Companies, Employer-sponsored Health Plans, and Healthcare Clearing Houses (all manage and transmit PHI)

Information Technology (IT) service providers that manage or store PHI for healthcare providers

Simplifying Security & Compliance
www.prescientsecurity.com

Learn More

HIPAA

7 Areas of HIPAA Compliance

	HIPAA Compliance Area	Description	Certification Process
1	Privacy Rule Adherence	Handling of patients' PHI	Internal audits, external audits, and compliance reviews
2	Security Rule Implementation	Protection of ePHI through safeguards	Security risk assessments, implementation of safeguards, and regular reviews
3	Risk Assessment and Management	Identifying and mitigating risks to ePHI	Conducting risk assessments, implementing risk management plans, and continuous monitoring
4	Employee Training and Cyber Awareness	Training employees on HIPAA policies and procedures	Regular training sessions, certification programs, and compliance checks
5	Breach Response and Notification	Responding to data breaches and notifying affected individuals	Developing and testing breach response plans, and maintaining notification procedures
6	Business Associate Agreements	Agreements with business associates handling PHI	Reviewing and updating agreements, and ensuring compliance with HIPAA requirements
7	Documentation and Audit Preparedness	Maintaining documentation and being prepared for audits	Keeping detailed records, conducting internal audits, and preparing for external audits

HIPAA vs PHIPA vs PIPEDA

HIPAA: Specific to the US and focuses on protecting health information within the healthcare sector, including providers, insurers, and business associates.

HiTech: A part of HIPAA, specific to the US, and focuses on the security of electronic health records.

PHIPA: Applies only within Ontario, Canada, governing how healthcare providers handle personal health information.

PIPEDA: Broader in scope and applies to all personal information collected, used, or disclosed in commercial activities by businesses across Canada, except in the provinces of Alberta, British Columbia, and Quebec.

Prescient Security and HIPAA, HiTech, PHIPA, and PIPEDA

For our HIPAA, PHIPA, and PIDEDA Services, we conduct thorough compliance assessments, develop risk management and mitigation strategy, create principled policies and training, provide ongoing support and advisement, and breach response and reporting tailored to HIPAA's federal standards in the U.S., PHIPA's Ontario-specific regulations, and PIPEDA's requirements across Canada.