

HIPAA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of regulations concerning the handling of health records.

The Office for Civil Rights (OCR) enforces three rules related to HIPAA:

1. HIPAA Privacy Rule, which protects the privacy of individually identifiable health information.
2. HIPAA Security Rule, which sets national standards for the security of electronic protected health information (ePHI).
3. HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information.

The Security Rule is designed to not only safeguard confidentiality of PHI but also ensures that the data you transmit or receive are not altered in the process and that the data in your information systems are available to appropriate individuals. The Security Rule is comprised of 3 main components:

- 1. ADMINISTRATIVE SAFEGUARDS -**
These safeguards address your operations. They include assigning responsibility to someone for security and having policies and procedures in place to direct your security efforts.
- 1. PHYSICAL SAFEGUARDS -**
These safeguards address physical and facility related matters such as locks and keys, where computers are located, how electronic media are disposed of, and generally how to make the environment safe.
- 2. TECHNICAL SAFEGUARDS -**
These safeguards are focused on controlling access to systems and electronic PHI. They identify who may have access to information systems, provide access to sets of data and specific functions in systems, audit persons who have used the systems, and protect the systems from malicious software.

Catapult enforces stringent security policies for protecting the privacy and confidentiality of user data. Along with best-in-class infrastructure, physical security and technical controls are adhered to to protect user information.

Catapult is neither considered a covered-entity or a Business Associate. Despite not being subject to HIPAA requirements, the organization has determined that given the nature

of the information ingested by the AMS platform, compliance with applicable HIPAA regulations is necessary.

An independent audit was conducted in August 2018 by The Kaplan Firm to review Catapult's processes and procedures. The report concluded that Catapult AMS is in compliance with HIPAA regulations for requirements deemed applicable to the AMS platform.