Maintaining HIPAA and HITECH Compliance While Using Cloudflare Products

If a company operates in the healthcare space (e.g. hospitals, laboratories, electronic health records, telemedicine platforms, health insurance providers etc.) in the United States, it may be subject to the U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. HIPAA and HITECH govern how companies may process and use individuals' protected health information (PHI).

While there is no formal validation for HIPAA or HITECH like there is for SOC 2, PCI, or ISO, Cloudflare's network, management infrastructure, and associated processes and procedures are consistent with many required or addressable privacy and security controls specified by HIPAA and related regulations. Examples of these controls include but are not limited to:

- Performing regular risk assessments and threat analysis against our controls and services
- A full suite of security, risk. and privacy policies that are reviewed on an annual basis
- Business Continuity and Disaster Recovery Plans
- Data encryption in transit and at rest
- Annual security and privacy training
- Breach notification procedures
- User authentication procedures including Multi Factor Authentication
- Internal audit policies and procedures related to monitoring IT safeguards

The requirements in the Security Rule around protecting PHI are very similar to requirements for protecting data for PCI, SOC 2, and ISO 27001. You can request copies of these validations through your account executive.

We offer a Business Associate Agreement (BAA) which incorporates the clauses required by HIPAA so that companies that are transmitting PHI can use Cloudflare security services and still meet their requirements. Some examples of services that may be in scope of HIPAA include CDN, WAF, and Bot Management. Some examples of services that may be outside of scope if purchased alone (would not merit a BAA) include Magic Transit and DNS.

Our BAA is only available for Enterprise-level customers with minimum spending thresholds and is non-negotiable since it merely reflects HIPAA regulations. Contact our sales team to learn more about using Cloudflare services while maintaining HIPAA compliance.