AMPCUS CYBER
Zero Trust Compliance Service Provider

HIPAA V/S GDPR

HIPAA	ASPECT	GDPR
United States	Jurisdiction	European Union (and EEA countries)
Announced in 1996, effective 2003 (Privacy Rule), 2005 (Security Rule).	Announced and Implemented	Adopted in 2016, enforced starting May 25, 2018.
Applies to healthcare entities like providers, plans, and clearinghouses.	Scope of Application	Applies to all organizations processing EU citizens' personal data, regardless of location.
PHI (Protected Health Information)	Protected Data	Personal Data (e.g., names, addresses, IPs) and Sensitive Data (health, biometrics, etc.).
Healthcare providers, health plans, and clearinghouses.	Covered Entities	Any organization handling EU citizens' personal data.
Not mandatory for all cases; treatment, payment, and operations are typically covered without explicit consent.	Consent	Requires clear, informed, and freely given consent for data processing unless other lawful bases apply.
Limited rights (e.g., accessing and requesting corrections to their health records).	Privacy Rights	Extensive rights, including access, correction, restriction, portability, and erasure (right to be forgotten).
Individuals can request access to their health records.	Right to Access	Individuals can access, correct, or receive copies of their data in a portable format.
Not applicable.	Right to be Forgotten	Explicit right to request data erasure under certain conditions.
Must notify affected individuals and HHS within 60 days of breach discovery.	Data Breach Reporting	Must notify supervisory authorities and affected individuals within 72 hours of breach discovery.
Not required under HIPAA, but organizations may appoint privacy and security officers.	Data Protection Officers	Required for certain organizations, especially those processing sensitive data at scale.
Up to $1.9 million annually, depending on violations.	Penalties for Non-Compliance	Up to €20 million or 4% of global annual turnover, whichever is higher.
Requires periodic risk analyses and mitigation under the Security Rule.	Assessments	Mandates Data Protection Impact Assessments (DPIAs) for high-risk data processing.
No specific data retention limit; determined by state laws or organizational policies.	Data Storage Requirements	Organizations should retain data only as long as necessary for its purpose.
Healthcare-specific privacy and security regulations.	Focus	Broad privacy regulation applicable to all industries.
No explicit rules for international data transfers.	Data Transfers	Strict regulations on transfers outside the EU (e.g., adequacy decisions).
U.S. Department of Health and Human Services (HHS).	Enforcement Authority	Data Protection Authorities (DPAs) in each EU country.
Privacy, Security, Breach Notification Rules.	Key Principles	Lawfulness, Fairness, Transparency, Data Minimization, Accountability, and Integrity.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com