Module 3 - Video 3 Summary: Data Privacy and Protection

Data Privacy

Preserving a data subject's information during any data transaction. It ensures trust and ethical use of data.

PII (Personally Identifiable Information)

Data that can uniquely identify an individual, such as email, address, phone number, and birthday. Must be safeguarded.

PHI (Protected Health Information)

Health-related data that can identify an individual, including diagnoses, treatments, and payment records.

GDPR (General Data Protection Regulation)

European privacy legislation regulating data collection, usage, and storage with strict compliance and reporting requirements.

Identity Access Management

A process that defines and restricts employee access to specific programs and datasets based on their roles.

NTK (Need to Know)

A principle where employees access only the minimum data necessary to perform their job duties.

Data Stewards

Internal privacy team responsible for monitoring and managing data access within an organization.

Audits

Formal examinations of data access to ensure safety, compliance, and to identify potential issues.

Security Keys

Physical or digital authentication methods used to verify user identity before accessing sensitive data.

Encryption

Encoding data into a secret format that can only be accessed with a digital key, protecting data during storage and transmission.