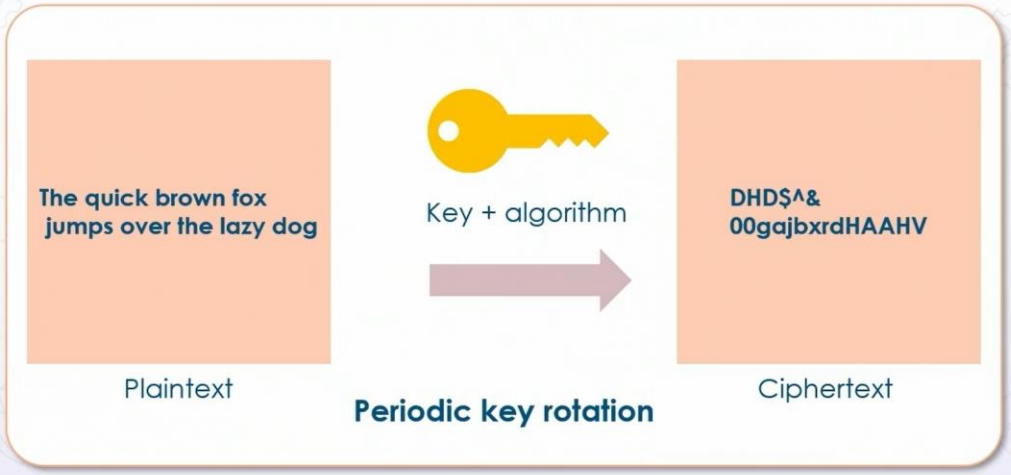
Sensitive Data Exposure Attacks

Legal and regulatory compliance

Encryption - Confidentiality



Hashing

- Ensures data integrity for messages
- Provides a secure method of storing passwords
- Detects file system modifications
- Can be used with encryption for confidentiality and integrity, and message authentication
- Is not reversible like encryption is

Hashing - Integrity

```
PS D:\> Get-Filehash .\Project_A.txt

Algorithm Hash                                                             Path
--------- ----                                                             ----
SHA256    E047A2E5625776671668BE7DE6029ABDC221E57DCFC4FEC3C5443CC1FBC65DBA D:\Project_A.txt
```

Hashing - Integrity

```
PS D:\> Get-Filehash .\Project_A.txt

Algorithm Hash                                                             Path
--------- ----                                                             ----
SHA256    E047A2E5625776671668BE7DE6029ABDC221E57DCFC4FEC3C5443CC1FBC65DBA D:\Project_A.txt
```

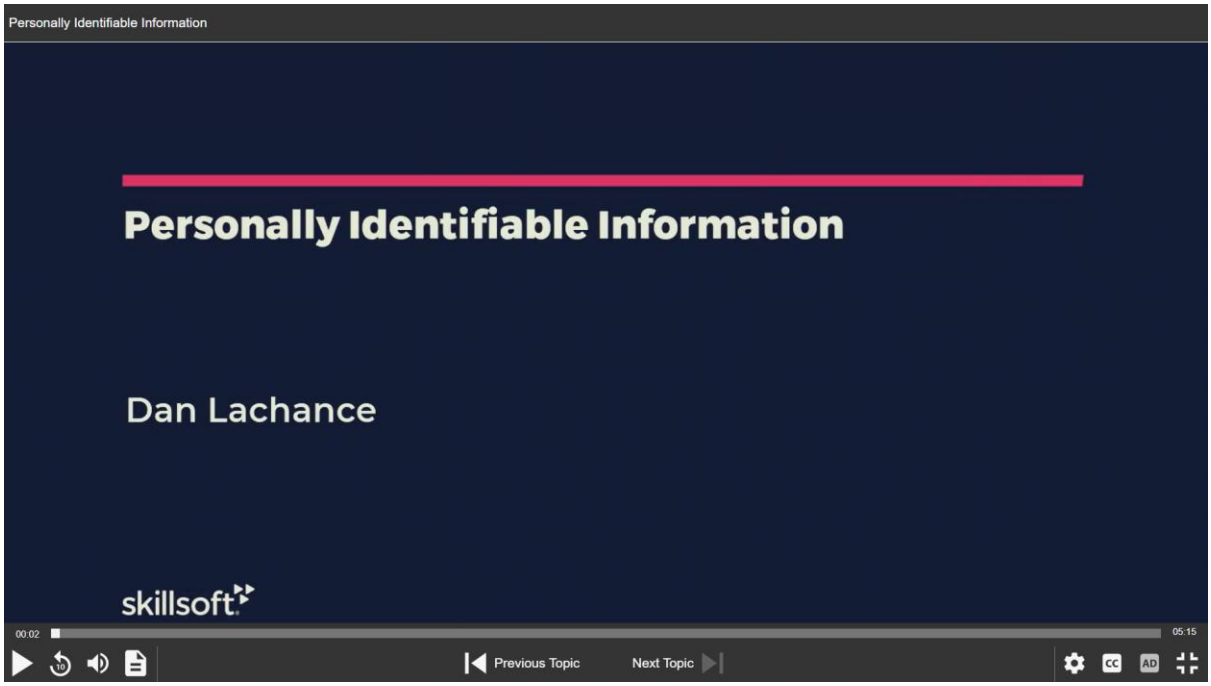
- Data is fed into a hashing algorithm
- A key is *not* used
- The output is a unique fixed-length representation of the input data
  - Hash
  - Message digest
- Modified data results in a different hash value
- File integrity monitoring (FIM)

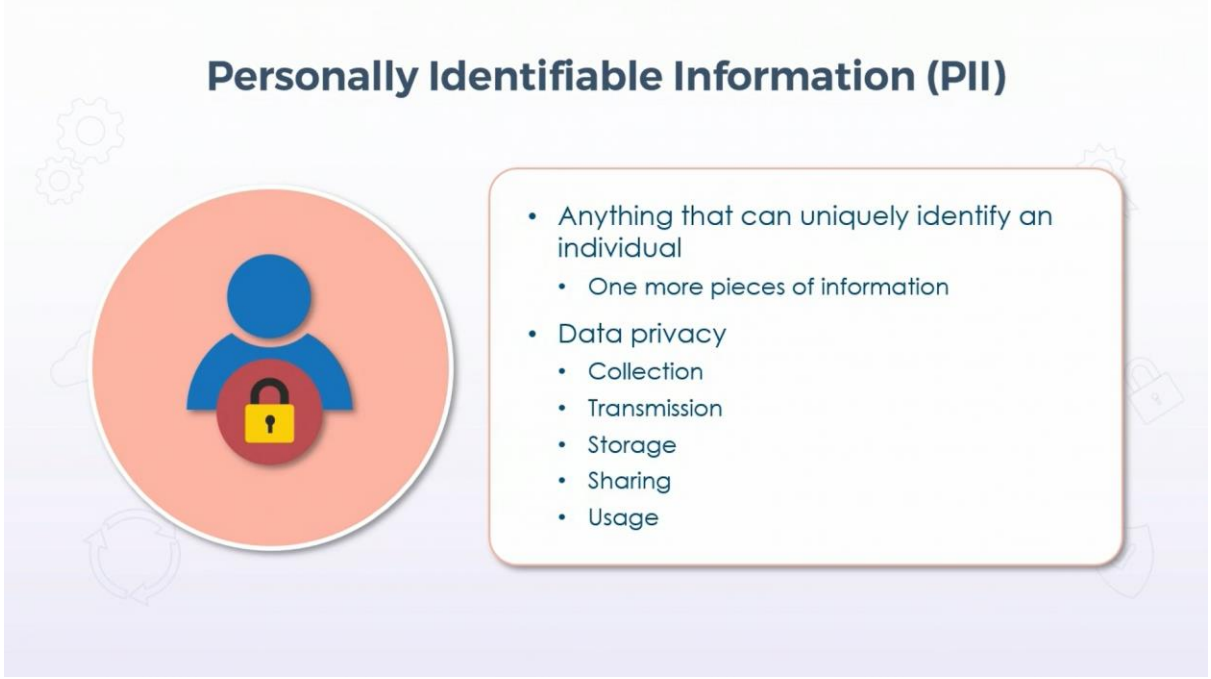
Hashing and Password Storage

```
uone@ubuntul : ~ $ sudo  tail  -1 /etc /shadow
Utwo : $6$yAl0Lvas3g8mT8Q1$H/x. WEWigXKWEn8U94D
qUybsrLYGMubfNMm/ : 18669 :0: 99999 : 7 : : :
```

- User passwords are hashed and stored in /etc/shadow
- Entering the correct password results in the exact same hash, which allows authentication
- Salting - add random data to password prior to hashing
- Unsalted hashes are easily cracked using rainbow tables

Cryptography and Storage


Personally Identifiable Information
Personally Identifiable Information
Dan Lachance
skillsoft
00:02
05:15
Previous Topic
Next Topic


Personally Identifiable Information (PII)
• Anything that can uniquely identify an individual
• One more pieces of information
• Data privacy
• Collection
• Transmission
• Storage
• Sharing
• Usage

Non-technology PII Examples

Mother's maiden name

Home street address

Credit card number

Technology PII Examples

IP address

Web browser cookie

Social media account

Sensitive Personal Information (SPI)

- Political party affiliation
- Sexual orientation or gender
- Trade union membership

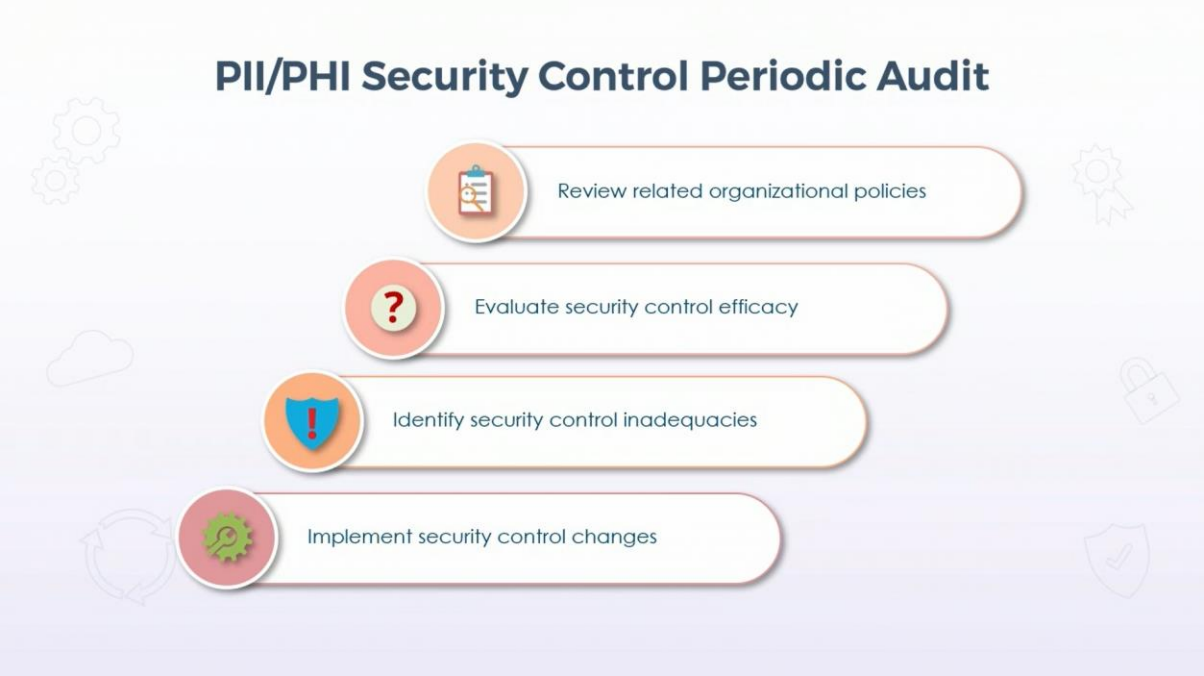
Protected Health Information (PHI)

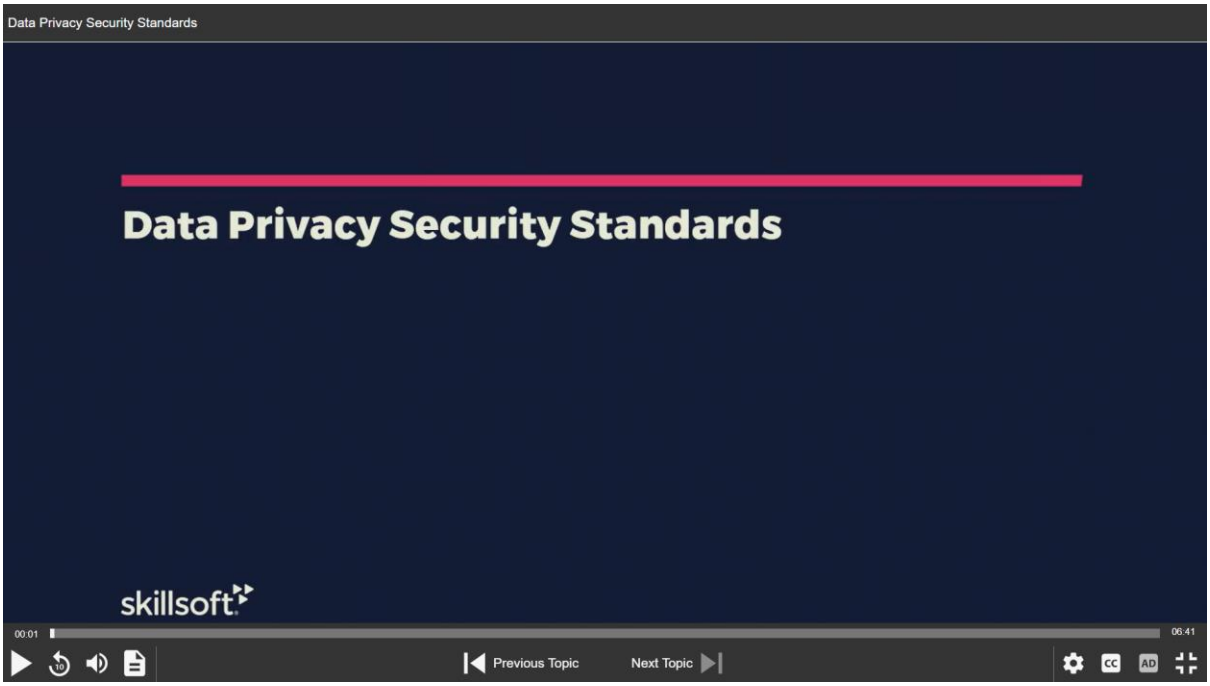
Similar to PII but focused on the medical industry in the U.S.

Past and current health information

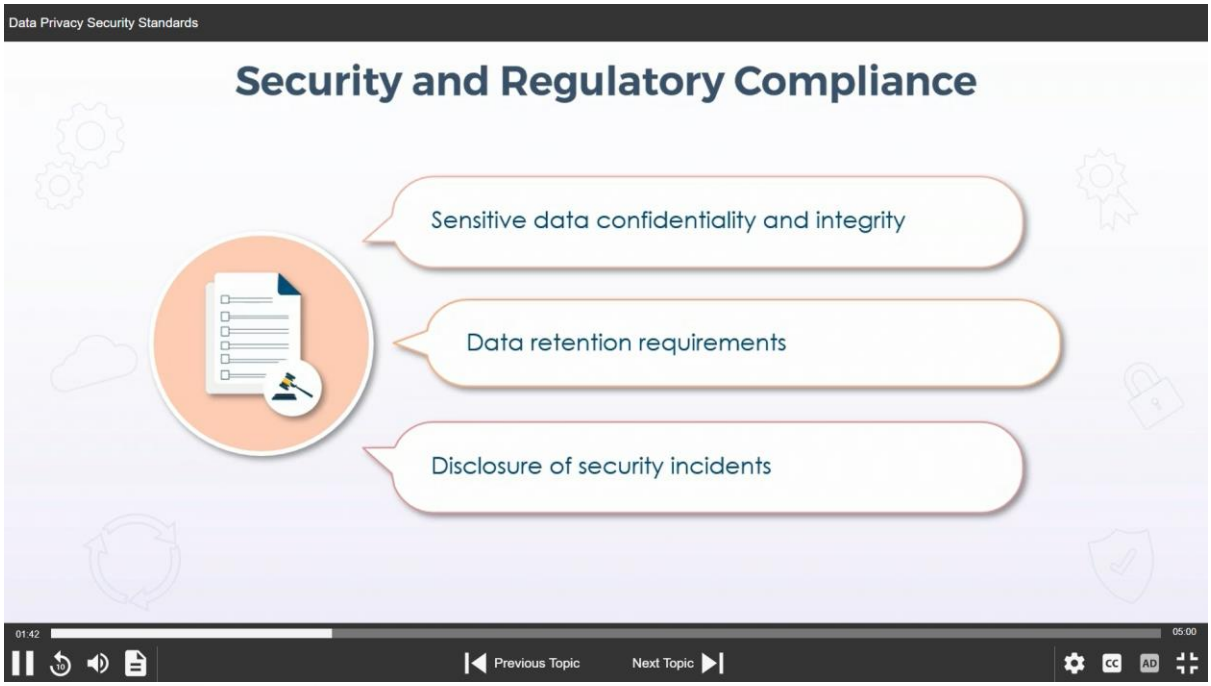
Future health details related to

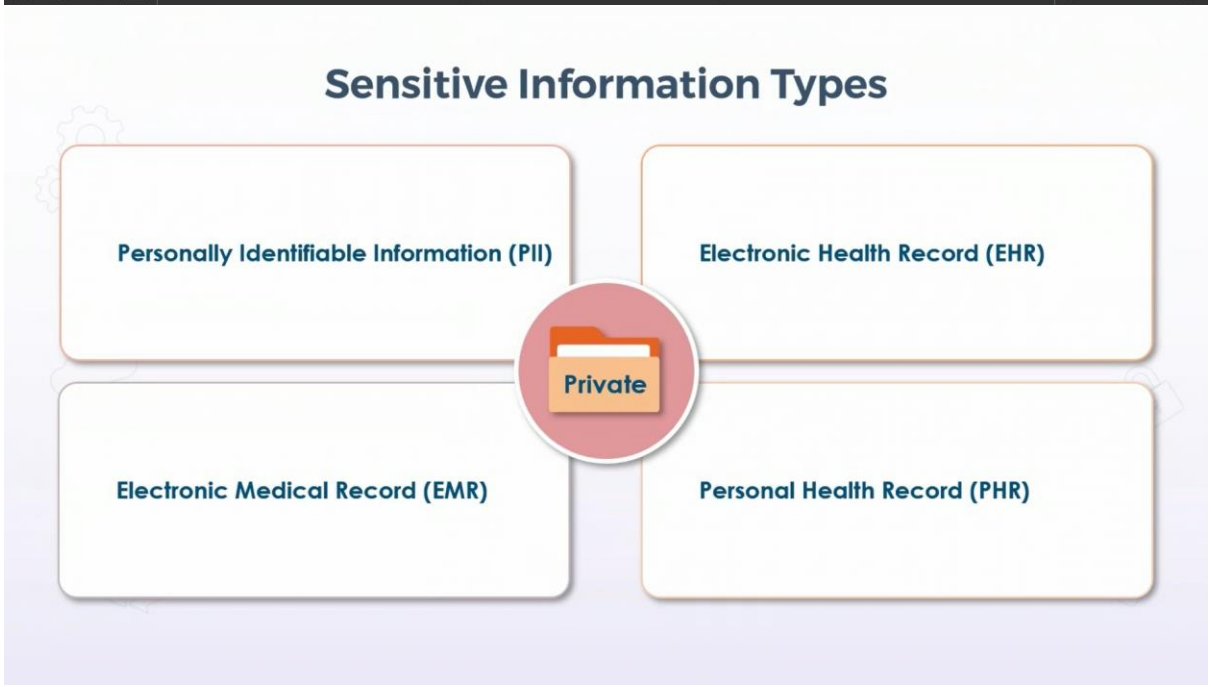
- Care
- Payment

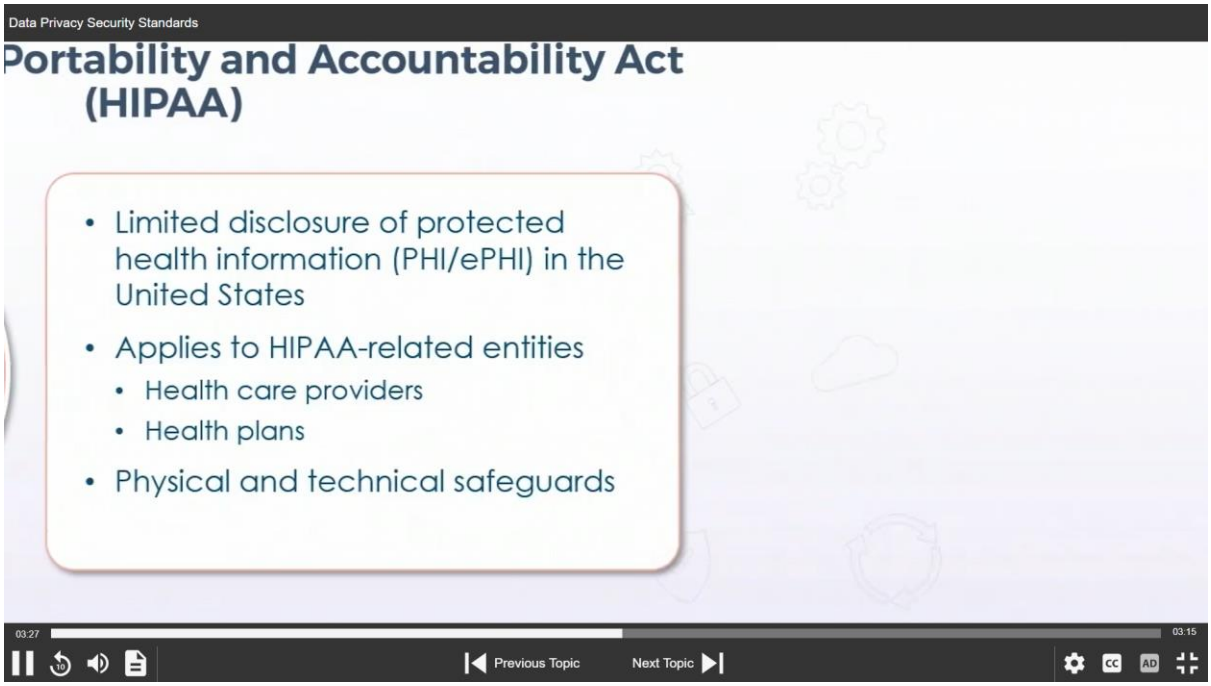

PII/PHI Security Control Periodic Audit
Review related organizational policies
Evaluate security control efficacy
Identify security control inadequacies
Implement security control changes


Data Privacy Security Standards
Data Privacy Security Standards
skillsoft
00:01
06:41
Previous Topic
Next Topic

Data Privacy Standards and Compliance


Data Privacy Security Standards
Security and Regulatory Compliance
Sensitive data confidentiality and integrity
Data retention requirements
Disclosure of security incidents
01:42
05:00
Previous Topic
Next Topic


Sensitive Information Types
Personally Identifiable Information (PII)
Electronic Health Record (EHR)
Private
Electronic Medical Record (EMR)
Personal Health Record (PHR)



General Data Protection Regulation (GDPR)

- **Legislative act of the European Union (EU)**
- **Puts control of personal data into the user's hands**
- **Data privacy of PII**
  - Collection and retention
  - Use
  - Sharing
- **Applies to organizations located anywhere**
- **EU citizens must provide consent, and have access to and the ability to correct their own personal information**

Children's Online Privacy Protection Act (COPPA)

American federal law requiring parental consent

Restricts Internet service information gathering related to children's personal information

nt Card Industry Data Security Standard (PCI DSS)

International

Each type of card's security recommendations differ slightly (Visa, Mastercard, etc.)

Merchant security standards for protecting cardholder data

PCI DSS Security Requirements

Goal	Control
Build and maintain a secure network	• Firewalls • Change system defaults
Protect cardholder data	• Storage data protection • Network encryption over open, public networks
Maintain a vulnerability management program	• Anti-virus solution including updates • Apply security to all SDLC phases
Implement strong access control	• 'Need to know basis' access to cardholder data • Unique user accounts • Physical security controls

Mitigating Sensitive Data Exposure Attacks

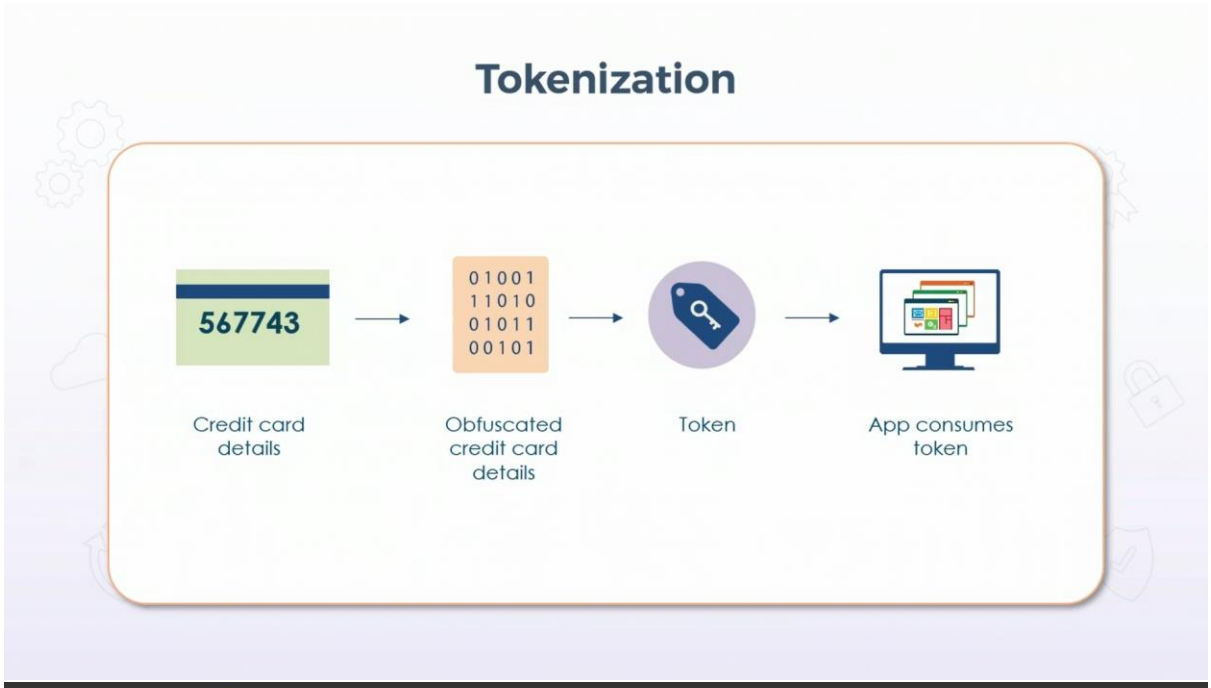
Data Classification

- Manual or automated metadata (labeling, tagging)
  - Files, folders, cloud resources, database records
- PII, financial, PHI, intellectual property (IP)
- Top secret, Confidential, etc.
- Microsoft File Server Resource Manager (FSRM), Amazon Macie

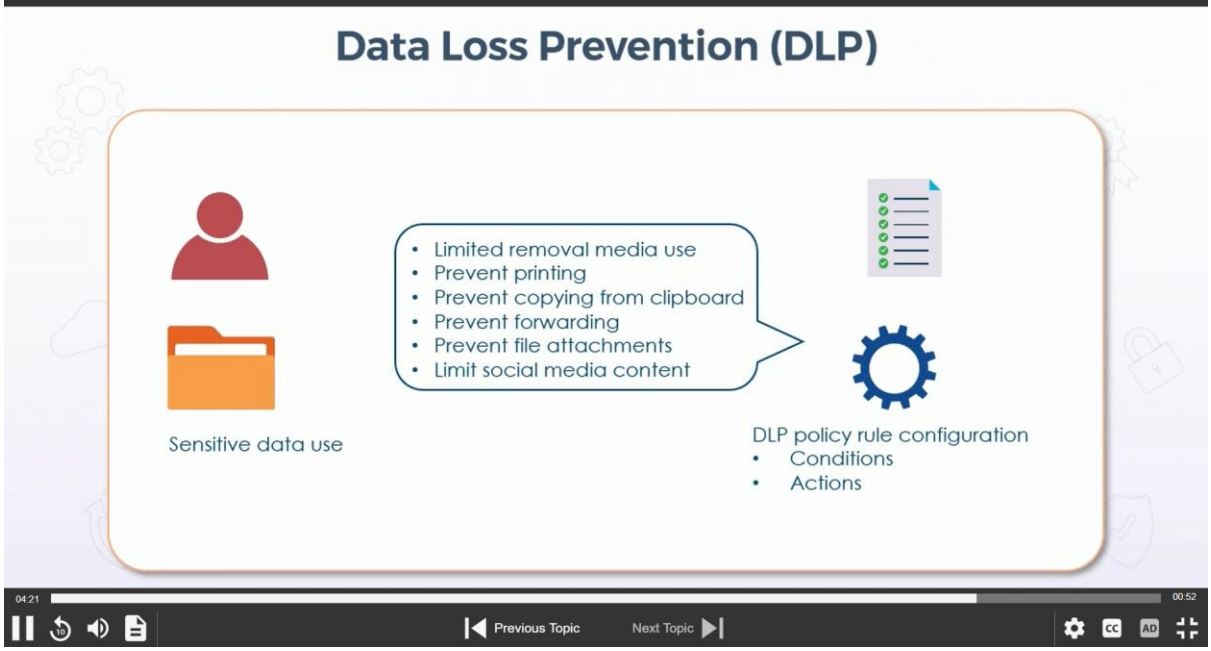
Sensitive Data Privacy

Anonymization

Masking



Mitigating Sensitive Data Exposure Attacks



Digital Rights Management (DRM)