[TITLE 45 – SUBTITLE A - Subchapter C - Part 164 3](#_Toc151458095)

[Subpart C - Security Standards for the Protection of Electronic Protected Health Information 3](#_Toc151458096)

[§ 164.302 Applicability. 3](#_Toc151458097)

[§ 164.304 Definitions. 3](#_Toc151458098)

[§ 164.306 Security standards: General rules. 3](#_Toc151458099)

[(a) General requirements. Covered entities and business associates must do the following: 3](#_Toc151458100)

[(b) Flexibility of approach: 3](#_Toc151458101)

[(c) Standards 3](#_Toc151458102)

[(d) Implementation specifications. 3](#_Toc151458103)

[(e) Maintenance 3](#_Toc151458104)

[§ 164.308 Administrative safeguards. 3](#_Toc151458105)

[(a) A covered entity or business associate must, in accordance with § 164.306: 3](#_Toc151458106)

[(b) 5](#_Toc151458107)

[§ 164.310 Physical safeguards. 5](#_Toc151458108)

[§ 164.312 Technical safeguards. 5](#_Toc151458109)

[(a) 5](#_Toc151458110)

[(b) Standard: Audit controls. 5](#_Toc151458111)

[(c) 5](#_Toc151458112)

[(d) Standard: Person or entity authentication 6](#_Toc151458113)

[(e) 6](#_Toc151458114)

[§ 164.314 Organizational requirements. 6](#_Toc151458115)

[§ 164.316 Policies and procedures and documentation requirements. 6](#_Toc151458116)

[§ 164.318 Compliance dates for the initial implementation of the security standards. 6](#_Toc151458117)

[Subpart E - Privacy of Individually Identifiable Health Information 6](#_Toc151458118)

[§ 164.500 Applicability. 6](#_Toc151458119)

[§ 164.501 Definitions. 6](#_Toc151458120)

[§ 164.502 Uses and disclosures of protected health information: General rules. 6](#_Toc151458121)

[§ 164.504 Uses and disclosures: Organizational requirements. 6](#_Toc151458122)

[§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. 7](#_Toc151458123)

[§ 164.508 Uses and disclosures for which an authorization is required. 7](#_Toc151458124)

[§ 164.510 Uses and disclosures for which an authorization is required. 7](#_Toc151458125)

[§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required. 7](#_Toc151458126)

[§ 164.514 Uses and disclosures for which an authorization or opportunity to agree or object is not required. 7](#_Toc151458127)

[§ 164.520 Notice of privacy practices for protected health information. 7](#_Toc151458128)

[§ 164.522 Rights to request privacy protection for protected health information. 7](#_Toc151458129)

[§ 164.524 Access of individuals to protected health information. 7](#_Toc151458130)

[§ 164.528 Accounting of disclosures of protected health information. 7](#_Toc151458131)

[§ 164.530 Administrative requirements. 7](#_Toc151458132)

[(a) 7](#_Toc151458133)

[(b) 7](#_Toc151458134)

[(c) 7](#_Toc151458135)

[(d) 8](#_Toc151458136)

[(e) 8](#_Toc151458137)

[(f) Standard: Mitigation 8](#_Toc151458138)

[(g) Standard: Refraining from intimidating or retaliatory acts 8](#_Toc151458139)

[(h) Standard: Waiver of rights 8](#_Toc151458140)

[(i) 8](#_Toc151458141)

[(j) 8](#_Toc151458142)

[(k) Standard: Group health plans 8](#_Toc151458143)

# TITLE 45 – SUBTITLE A - Subchapter C - Part 164

## Subpart C - Security Standards for the Protection of Electronic Protected Health Information

### § 164.302 Applicability.

Does not apply.

### § 164.304 Definitions.

Does not apply.

### § 164.306 Security standards: General rules.

#### General requirements. Covered entities and business associates must do the following:

Does not apply.

#### Flexibility of approach:

Does not apply.

#### Standards

Does not apply.

#### Implementation specifications.

Does not apply.

#### Maintenance

Does not apply.

### § 164.308 Administrative safeguards.

#### A covered entity or business associate must, in accordance with [§ 164.306](https://www.ecfr.gov/current/title-45/section-164.306):

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
   1. **Standard: Security management process:**

Implement policies and procedures to prevent, detect, contain, and correct security violations

* 1. **Implementation specifications:**
     1. **Risk analysis (Required).**

Does not apply

* + 1. **Risk management (Required)**

Does not apply

* + 1. **Sanction policy (Required)**

Does not apply.

* + 1. **Information system activity review (Required)**

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

1. **Standard:** Assigned security responsibility.

Does not apply

1. 1. **Standard: Workforce security:**

Does not apply

* 1. **Implementation specifications:**

1. **Authorization and/or supervision (Addressable)**

Does not apply.

1. **Authorization and/or supervision (Addressable)**

Does not apply.

1. **Termination procedures (Addressable)**

Does not apply.

* 1. **Standard: Information access management:**

Does not apply

* 1. **Implementation specifications:**

1. **Isolating health care clearinghouse functions (Required)**

Does not apply.

1. **Access authorization (Addressable).**

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

1. **Access establishment and modification (Addressable)**

Does not apply.

* 1. **Standard: Security awareness and training:**

Does not apply

* 1. **Implementation specifications. Implement:**

1. **Security reminders (Addressable)**

Periodic security updates.

1. **Protection from malicious software (Addressable)**

Does not apply.

1. **Log-in monitoring (Addressable)**

Procedures for monitoring log-in attempts and reporting discrepancies.

1. **Password management (Addressable)**

Procedures for creating, changing, and safeguarding passwords.

* 1. **Standard: Security incident procedures:**

Does not apply

* 1. **Implementation specifications: Response and reporting (Required):**

Does not apply

* 1. **Standard: Contingency plan:**

Does not apply

* 1. **Implementation specifications:**

Does not apply.

1. **Standard: Evaluation**

Does not apply

#### 

1. **Business associate contracts and other arrangements**.

Does not apply

1. **A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information**.

Does not apply

1. **Implementation specifications: Written contract or other arrangement (Required).**

Does not apply

### § 164.310 Physical safeguards.

Does not apply.

### § 164.312 Technical safeguards.

#### 

1. **Standard: Access control**. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)
2. **Implementation specifications:**
   1. **Unique user identification (Required).**

Assign a unique name and/or number for identifying and tracking user identity.

* 1. **Emergency access procedure (Required):**

Does not apply.

* 1. **Automatic logoff (Addressable):**

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

* 1. **Encryption and decryption (Addressable):**

Implement a mechanism to encrypt and decrypt electronic protected health information.

#### Standard: Audit controls.

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

#### 

1. **Standard: integrity**.

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

1. **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)**.

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

#### Standard: Person or entity authentication

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

#### 

1. **Standard: Transmission security**.

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

1. **Implementation specifications:**
2. **Integrity controls (Addressable).**

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

1. **Encryption (Addressable):**

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate

### § 164.314 Organizational requirements.

Does not apply.

### § 164.316 Policies and procedures and documentation requirements.

Does not apply.

### § 164.318 Compliance dates for the initial implementation of the security standards.

Does not apply.

## Subpart E - Privacy of Individually Identifiable Health Information

### § 164.500 Applicability.

Does not apply.

### § 164.501 Definitions.

Does not apply.

### § 164.502 Uses and disclosures of protected health information: General rules.

Does not apply.

### § 164.504 Uses and disclosures: Organizational requirements.

Does not apply

### § 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

Does not apply

### § 164.508 Uses and disclosures for which an authorization is required.

Does not apply.

### § 164.510 Uses and disclosures for which an authorization is required.

Does not apply.

### § 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

Does not apply.

### § 164.514 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

Does not apply.

### § 164.520 Notice of privacy practices for protected health information.

Does not apply.

### § 164.522 Rights to request privacy protection for protected health information.

Does not apply.

### § 164.524 Access of individuals to protected health information.

Does not apply.

### § 164.528 Accounting of disclosures of protected health information.

Does not apply.

### § 164.530 Administrative requirements.

#### 

1. **Standard: Personnel designations**.

Does not apply

1. **Implementation specification: Personnel designations:**

Does not apply

#### 

1. **Standard: Training**

Does not apply

1. **Implementation specifications: Training.**

Does not apply

#### 

1. **Standard: Safeguards**.

Does not apply

2. **Implementation specification: Safeguards**

Does not apply.

Does not apply

#### 

Does not apply

#### 

Does not apply

#### Standard: Mitigation

Does not apply

#### Standard: Refraining from intimidating or retaliatory acts

Does not apply

#### Standard: Waiver of rights

Does not apply

#### 

Does not apply

#### 

Does not apply

#### Standard: Group health plans

Does not apply