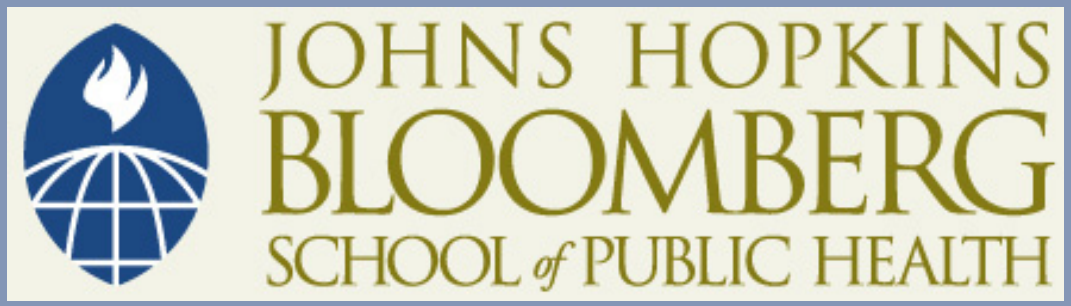

JOHNS HOPKINS
UNIVERSITY

Section D

Health Information Security

Basic Concepts

- What is **privacy** (of health information)?
  - An individual's (or organization's) right to determine whether, what, when, by whom, and for what purpose their personal health information is collected, accessed, used, or disclosed

- What is **security** (of health information)?
  - A defined set of administrative, physical, and technical actions used or taken to protect the confidentiality, availability, and integrity of health information

Source: HITSP vocabulary—modified and expanded from 45 CFR 164.304.

Basic Information Security Concepts

- **Confidentiality**
  - The property that data or information is not made available or disclosed to unauthorized persons or processes

- **Integrity**
  - The property that data or information has not been altered or destroyed in an unauthorized manner

- **Availability**
  - The property that data or information is accessible and usable upon demand by an authorized person

Source: 45 CFR 164.304.

Base Requirements and Principles

- **Information security**
  - Multiple industry applicability—not "specific" to health care
  - Extensive experience and "standards" in other industries and in health care
  - Less regulatory controls: only limited number of federal and state laws and regulations
  - No national framework for health information in place
  - "80% policies and procedures, 20% technology"

Base Requirements and Principles

- **HIPAA security rule**
  - Main goal: to protect the confidentiality, integrity, and availability of electronic protected health information
  - Limited to covered entities and e-PHI
  - Requirements are scalable : can (and must) be implemented regardless of size, location
  - Technology-neutral: no specific technology standards called upon
  - Comprehensive: administrative, physical, technical safeguard requirements
  - Some specifications are required, some are “addressable”

Section I: Administrative Safeguards

SECTION I - ADMINISTRATIVE SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.308(a)(1)	Security Management Process	Risk analysis	(R)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
		Risk management	(R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
		Sanction policy	(R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
		Information system activity Review	(R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
164.308(a)(2	Assigned Security Responsibility	Security Official	(R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
164.308(a)(3)	Workforce security	Authorization and/or supervision	(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
		Workforce clearance procedure	(A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
		Termination procedure	(A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

Source: US Dept of Health and Human Services

Section I: Administrative Safeguards

SECTION I - ADMINISTRATIVE SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.308(a)(1)	Security Management Process	Risk analysis	(R)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
		Risk management	(R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
		Sanction policy	(R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
		Information system activity Review	(R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
164.308(a)(2	Assigned Security Responsibility	Security Official	(R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
164.308(a)(3)	Workforce security	Authorization and/or supervision	(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
		Workforce clearance procedure	(A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
		Termination procedure	(A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

Source: US Dept of Health and Human Services

Section I: Administrative Safeguards

SECTION I - ADMINISTRATIVE SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.308(a)(1)	Security Management Process	Risk analysis	(R)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
		Risk management	(R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
		Sanction policy	(R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
		Information system activity Review	(R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
164.308(a)(2	Assigned Security Responsibility	Security Official	(R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
164.308(a)(3)	Workforce security	Authorization and/or supervision	(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
		Workforce clearance procedure	(A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
		Termination procedure	(A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

Source: US Dept of Health and Human Services

Section I: Administrative Safeguards

SECTION I - ADMINISTRATIVE SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.308(a)(4)	Information access management	Isolating healthcare clearinghouse function	(R)	If a health care clearinghouse is part of a larger organization, the Clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
		Access authorization	(A)	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.
		Access establishment and modification	(A)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
164.308(a)(5)	Security awareness and training	Security reminders	(A)	Provide periodic security updates.
		Protection from malicious software	(A)	Procedures for guarding against, detecting, and reporting malicious software.
		Log-in monitoring	(A)	Procedures for monitoring log-in attempts and reporting discrepancies.
		Password management	(A)	Procedures for creating, changing, and safeguarding passwords.
164.308(a)(6)	Security incident procedures	Response and reporting	(R)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Source: US Dept of Health and Human Services

Section I: Administrative Safeguards

SECTION I - ADMINISTRATIVE SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.308(a)(7)	Contingency plan	Data back-up plan	(R)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
		Disaster recovery plan	(R)	Establish (and implement as needed) procedures to restore any loss of data.
		Emergency mode operation plan	(R)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
		Testing and revision procedure	(A)	Implement procedures for periodic testing and revision of contingency plans.
		Applications and data criticality analysis	(A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.
164.308(a)(8)	Evaluation	Technical and non-technical evaluation	(R)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
164.308(b)(1)	Business associate contracts and other arrangements	Written contract or other arrangement	(R)	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

Source: US Dept of Health and Human Services

Section II: Physical Safeguards

SECTION II - PHYSICAL SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.310(a)(1)	Facility access controls	Contingency operations	(A)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		Facility security plan	(A)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		Access control and validation procedures	(A)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		Maintenance records	(A)	Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (e.g., hardware, walls, doors, locks).
164.310(b)	Workstation use	Function and attributes	(R)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.
164.310(c)	Workstation security	Restrict access	(R)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
164.310(d)(1)	Device and media controls	Disposal	(R)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		Media re-use	(R)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		Accountability	(A)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		Data back-up and storage	(A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Source: US Dept of Health and Human Services

Section III: Technical Safeguards

SECTION III - TECHNICAL SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.312(a)(1	Access control	Unique user identification	(R)	Assign a unique name and/or number for identifying and tracking user identity.
		Emergency access procedure	(R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		Automatic log-off	(A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		Encryption and decryption	(A)	Implement a mechanism to encrypt and decrypt electronic protected health information.
164.312(b)	Audit controls		(R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
164.312(c)	Integrity	Mechanism to authenticate electronic protected health information	(A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
164.312(d)	Person or entity authentication		(R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
164.312(e)(1)	Transmission security	Integrity controls	(A)	An implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
		Encryption	(A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Source: US Dept of Health and Human Services

Section III: Technical Safeguards

SECTION III - TECHNICAL SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.312(a)(1	Access control	Unique user identification	(R)	Assign a unique name and/or number for identifying and tracking user identity.
		Emergency access procedure	(R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		Automatic log-off	(A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		Encryption and decryption	(A)	Implement a mechanism to encrypt and decrypt electronic protected health information.
164.312(b)	Audit controls		(R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
164.312(c)	Integrity	Mechanism to authenticate electronic protected health information	(A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
164.312(d)	Person or entity authentication		(R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
164.312(e)(1)	Transmission security	Integrity controls	(A)	An implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
		Encryption	(A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Source: US Dept of Health and Human Services

Section III: Technical Safeguards

SECTION III - TECHNICAL SAFEGUARDS				
Citation	**Standard**	**Implementation Specifications (R) = Required; (A) = Addressable**		**Description**
164.312(a)(1	Access control	Unique user identification	(R)	Assign a unique name and/or number for identifying and tracking user identity.
		Emergency access procedure	(R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		Automatic log-off	(A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		Encryption and decryption	(A)	Implement a mechanism to encrypt and decrypt electronic protected health information.
164.312(b)	Audit controls		(R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
164.312(c)	Integrity	Mechanism to authenticate electronic protected health information	(A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
164.312(d)	Person or entity authentication		(R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
164.312(e)(1)	Transmission security	Integrity controls	(A)	An implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
		Encryption	(A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Source: US Dept of Health and Human Services

Security Standards for e-Health

- Main focus
  - User identification: management of identity credentials
    - Establishing unique identity of a user
  - Authentication: identity proofing
    - Verifying that an individual/entity is who he/she/it claims
  - Authorization
    - Establishing the type of actions an individual/entity can do, upon being authenticated
  - Access control
    - Controlling the type of actions an individual/entity can do, upon being authenticated

Security Standards for e-Health

- Main focus
  - Non-repudiation
    - Verification that the sender and recipient were, in fact, who they claim to be
  - Audit trails and controls
    - Establishing mechanisms to collect, maintain, and monitor events related to health information and take action
  - Secure communication
    - Ensuring that end-to-end connections used to transmit health information are secured from intrusions
  - Consistent time
    - Ensuring that the reference time used by systems is consistent

ARRA and Interoperable Security Standards

- Under ARRA, HHS established standards and certification criteria for EHR technology to ensure personal health information is protected

- Standards intended to address issues of:
  - Access control
  - Audit
  - Authentication
  - Consent management
  - Consistent time
  - Identity management
  - Non-repudiation
  - De-identification
  - Secure transmission
  - Secure email

Final Regulations

Final Regulations on Security-Related Standards and Certification Criteria for MU-2010

Security Standards to protect health information created, maintained, and exchanged - § 170.210

Area	Standard
§ 170.210(a) Encryption and decryption of electronic health information	General: Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 Exchange: Any encrypted and integrity protected link
§ 170.210(b) Record actions related to electronic health information	The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.
§ 170.210(c) Verification that electronic health information has not been altered in transit	A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October, 2008)) must be used to verify that electronic health information has not been altered.
§ 170.210(d) Record TPO Disclosures	The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.

Source: CMS Centers for Medicare and Medicaid Services

Final Regulations

Final Regulations on Security-Related Standards and Certification Criteria for MU-2010

Security Certification Criteria for Complete EHRs and EHR Modules - § 170.302

Topic	Certification Criteria (Interim Rule)	Certification Criteria (Final Rule)	Standard and Implementation Specifications (Final Rule)
Meaningful Use Stage 1 Objective: Protect electronic health information created or maintained by the certified EHR technology			
Meaningful Use Stage 1 Measure: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process			
Topic: Access Control	Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.	§170.302(o) Unchanged	N/A
Topic: Emergency Access	Emergency access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	§170.302(p) Unchanged	N/A
Topic: Automatic Log-off	Automatic log-off. Terminate an electronic session after a predetermined time of inactivity.	§170.302(q) Unchanged	N/A
Topic: Audit Log	(1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Alerts. Provide alerts based on user-defined events. (3) Display and print. Electronically display and print all or a specified set of recorded information upon request or at a set period of time.	§170.302(r) (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210(b).	(b) Record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

Source: CMS Centers for Medicare and Medicaid Services

Final Regulations

Final Regulations on Security-Related Standards and Certification Criteria for MU-2010

Security Certification Criteria for Complete EHRs and EHR Modules - § 170.302

Topic	Certification Criteria (Interim Rule)	Certification Criteria (Final Rule)	Standard and Implementation Specifications (Final Rule)
Meaningful Use Stage 1 Objective: Protect electronic health information created or maintained by the certified EHR technology			
Meaningful Use Stage 1 Measure: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process			
Topic: Access Control	Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.	§170.302(o) Unchanged	N/A
Topic: Emergency Access	Emergency access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	§170.302(p) Unchanged	N/A
Topic: Automatic Log-off	Automatic log-off. Terminate an electronic session after a predetermined time of inactivity.	§170.302(q) Unchanged	N/A
Topic: Audit Log	(1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Alerts. Provide alerts based on user-defined events. (3) Display and print. Electronically display and print all or a specified set of recorded information upon request or at a set period of time.	§170.302(r) (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210(b).	(b) Record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

Source: CMS Centers for Medicare and Medicaid Services

Final Regulations

Final Regulations on Security-Related Standards and Certification Criteria for MU-2010

Security Certification Criteria for Complete EHRs and EHR Modules - § 170.302

Topic	Certification Criteria (Interim Rule)	Certification Criteria (Final Rule)	Standard and Implementation Specifications (Final Rule)
Meaningful Use Stage 1 Objective: Protect electronic health information created or maintained by the certified EHR technology			
Meaningful Use Stage 1 Measure: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process			
Topic: Access Control	Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.	§170.302(o) Unchanged	N/A
Topic: Emergency Access	Emergency access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	§170.302(p) Unchanged	N/A
Topic: Automatic Log-off	Automatic log-off. Terminate an electronic session after a predetermined time of inactivity.	§170.302(q) Unchanged	N/A
Topic: Audit Log	(1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Alerts. Provide alerts based on user-defined events. (3) Display and print. Electronically display and print all or a specified set of recorded information upon request or at a set period of time.	§170.302(r) (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210(b).	(b) Record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

Source: CMS Centers for Medicare and Medicaid Services

Final Regulations

Final Regulations on Security-Related Standards and Certification Criteria for MU-2010

Topic	Certification Criteria (Interim Rule)	Certification Criteria (Final Rule)	Standard and Implementation Specifications (Final Rule)
Meaningful Use Stage 1 Objective: Protect electronic health information created or maintained by the certified EHR technology			
Meaningful Use Stage 1 Measure: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process			
Topic: Integrity	(1)In transit. Verify that electronic health information has not been altered in transit in accordance with the standard specified in §170.210(c). (2) Detection. Detect the alteration and deletion of electronic health information and audit logs, in accordance with the standard specified in §170.210(c).	§170.302(s) (1) Create a message digest in accordance with the standard specified in 170.210(c). (2) Verify in accordance with the standard specified in 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered. (3) Detection. Detect the alteration of audit logs.	c) Verification that electronic health information has not been altered in transit. Standard. A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October, 2008)) must be used to verify that electronic health information has not been altered.
Topic: Authentication	(1) Local. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. (2) Cross network. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in §170.210(d).	§170.302(t) Authentication. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.	N/A

Source: CMS Centers for Medicare and Medicaid Services

Final Regulations

Final Regulations on Security-Related Standards and Certification Criteria for MU-2010

Topic	Certification Criteria (Interim Rule)	Certification Criteria (Final Rule)	Standard and Implementation Specifications (Final Rule)
Meaningful Use Stage 1 Objective: Protect electronic health information created or maintained by the certified EHR technology			
Meaningful Use Stage 1 Measure: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process			
Topic: Encryption	(1) General. Encrypt and decrypt electronic health information according to user-defined preferences in accordance with the standard specified in §170.210(a)(1). (2) Exchange. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).	§170.302(u) General encryption. Encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for Certified EHR Technology. §170.302(v) Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).	(a)(1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2. (a)(2) Exchange. Any encrypted and integrity protected link.
Topic: Accounting of Disclosures	Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(e).	§170.302(w) Certification criterion made optional, while the text of this certification criterion remains unchanged	(d) Record treatment, payment, and health care operations disclosures. The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.

Source: CMS Centers for Medicare and Medicaid Services

Summary

- HIPAA has provided a comprehensive framework for health information security

- The regulations on Standards and Certification Criteria for Meaningful Use begin to expand this framework into the EHRs and HIEs arena

Summary

- Many challenges remain:
  - Cross-jurisdictional/cross-entity authentication of all users (patient, provider, systems, others)
  - Authorization/access control
  - Audit
  - Nonrepudiation
  - Attribution of source
  - Sequestration of segmented data
  - Implementation of the expanded accounting of disclosures requirements

- Work is being done by various national committees, working groups, and project teams to address these issues