(C) Emergency mode operation plan
(Required). Establish (and implement as needed) procedures to enable con-
tinuation of critical business processes for protection of the security of elec-
tronic protected health information while operating in emergency mode.

(D) Testing and revision procedures
(Addressable). Implement procedures for periodic testing and revision of con-
tingency plans.

(E) Applications and data criticality
analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform a
periodic technical and nontechnical evaluation, based initially upon the
standards implemented under this rule and subsequently, in response to envi-
ronmental or operational changes affecting the security of electronic pro-
tected health information, that establishes the extent to which an entity’s
security policies and procedures meet the requirements of this subpart.

(b)(1) Standard: Business associate con-
tracts and other arrangements. A covered
entity, in accordance with §164.306, may permit a business associate to cre-
ate, receive, maintain, or transmit electronic protected health information
on the covered entity’s behalf only if the covered entity obtains satisfac-
tory assurances, in accordance with §164.314(a) that the business associate
will appropriately safeguard the information.

(2) This standard does not apply with
respect to—

(i) The transmission by a covered en-
tity of electronic protected health informa-
tion to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a
group health plan or an HMO or health insurance issuer on behalf of a group
health plan to a plan sponsor, to the extent that the requirements of
§164.314(b) and §164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or
to other agencies providing the services at §164.502(e)(1)(ii)(C), when the
covered entity is a health plan that is a government program providing pub-
lic benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the
satisfactory assurances it provided as a business associate of another covered
entity will be in noncompliance with the standards, implementation spec-
ifications, and requirements of this paragraph and §164.314(a).

(4) Implementation specifications: Written
contract or other arrangement (Re-
quired). Document the satisfactory assur-
ances required by paragraph (b)(1) of
this section through a written contract
or other arrangement with the business
associate that meets the applicable re-
quirements of §164.314(a).

§164.310 Physical safeguards.
A covered entity must, in accordance
with §164.306:

(a)(1) Standard: Facility access con-
trols. Implement policies and proce-
dures to limit physical access to its electronic information systems and the
facility or facilities in which they are housed, while ensuring that properly
authorized access is allowed.

(b)(1) Standard: Business associate con-
tracts and other arrangements. A covered
entity, in accordance with §164.306, may permit a business associate to cre-
ate, receive, maintain, or transmit electronic protected health information
on the covered entity’s behalf only if the covered entity obtains satisfac-
tory assurances, in accordance with §164.314(a) that the business associate
will appropriately safeguard the information.

(2) This standard does not apply with
respect to—

(i) The transmission by a covered en-
tity of electronic protected health informa-
tion to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a
group health plan or an HMO or health insurance issuer on behalf of a group
health plan to a plan sponsor, to the extent that the requirements of
§164.314(b) and §164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or
to other agencies providing the services at §164.502(e)(1)(ii)(C), when the
covered entity is a health plan that is a government program providing pub-
lic benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the
satisfactory assurances it provided as a business associate of another covered
entity will be in noncompliance with the standards, implementation spec-
ifications, and requirements of this paragraph and §164.314(a).

(4) Implementation specifications: Written
contract or other arrangement (Re-
quired). Document the satisfactory assur-
ances required by paragraph (b)(1) of
this section through a written contract
or other arrangement with the business
associate that meets the applicable re-
quirements of §164.314(a).
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 protected health information.  
(c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications:
(i) Disposal (Required). 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.
(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 164.312 Technical safeguards.

A covered entity must, in accordance with §164.306:

(a)(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:
(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) 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.

(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) 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.

(d) 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.

(e)(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.

(2) Implementation specifications:
(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

§ 164.314 Organizational requirements.

(a)(1) Standard: Business associate contracts or other arrangements. (i) The contract or other arrangement between