24BY7 SECURITY

Cybersecurity and Compliance Specialists

www.24by7security.com

SubPart-C

Security Standards for Protection of ePHI

164.308 Administrative Safeguards

A Covered Entity or Business Associate must:

- ☐ Implement Security management process (S)
- ☐ Conduct periodic risk analysis (R)
- ☐ Implement Risk management (R)
- ☐ Apply sanction policies (R)
- ☐ Information system activity review (R)
- ☐ Assign security official (S)
- ☐ Workforce security (S)
- ☐ Information access management (S)
- ☐ Security awareness training program (S)
- ☐ Security incident procedures (S)
- ☐ Establish contingency plan – Backup & Emergency Mode (R)
- ☐ Establish BA contracts (S)

164.310 Physical Safeguards

A Covered Entity or Business Associate must:

- ☐ Implement contingency operations (A)
- ☐ Safeguard Facility and Equipment (A)
- ☐ Access Control and Validate procedures (A)
- ☐ Document maintenance record of repair (A)
- ☐ Implement safeguards for workstation use and security (S)
- ☐ Log receipt and removal of hardware and electronic media into/out/within the facility (S)

164.312 Technical Safeguards

A Covered Entity or Business Associate must have:

- ☐ **Access Controls** - authorized personnel to access ePHI (S)
- ☐ **Audit Controls** - record and examine access and other activity in information system (S)
- ☐ **Integrity Controls** - ePHI is not altered or destroyed (S)
- ☐ **Transmission Security** - guard against unauthorized access to ePHI that is being transmitted over an electronic network (S)

S=Standards, A=Addressable, R=Required

164.316 Policies, Procedures, Documentation Requirement

A Covered Entity or Business Associate must:

- ☐ Implement policies and procedures,document it (S)
- ☐ Retain the documentation for 6 years from the date of its creation, or date when it last was in effect, whichever is later (R)
- ☐ Make documentation available to one who is responsible for implementing procedures to which documentation pertains (R)
- ☐ Review documentation periodically and update as needed (R)

SubPart-D

(Notification in the case of Unsecured ePHI Disclosure)

164.400 – 164.414 Notification to HHS in the case of Unsecured ePHI

A CE should notify:

- ☐ Each Individual - in writing no later than 60 days after discovery of breach, with brief description in plain language.
- ☐ Media - for breach involving more than 500 individuals no later than 60 days.
- ☐ Secretary – For breaches involving less than 500 individuals CE should maintain a log or other documentation, and for more than 500 should provide the notification as mentioned on HHS website.

BA should notify:

- ☐ CE of the breach no later than 60 days after discovery, with the notice identifying each individual.

Law Enforcement Delay:

- ☐ If a Law enforcement official mentions orally/writing to delay the notification of the breach, CE/BA should delay accordingly.

Burden of Proof:

- ☐ CE/BA shall have the burden of demonstrating that all the notifications were made as required or that the use or disclosure did not constitute a breach.

SECURITY & PRIVACY REGULATIONS

SubPart-E

(Privacy of Individually Identifiable Health Information)

164.502
Uses and disclosures of PHI

(a) Standard: A CE/BA may not use or disclose PHI except as permitted or required
- (1) Permitted: A CE is permitted to use or disclose PHI :
  - (i) To individual
  - (ii) For treatment, payment, or healthcare operations
  - (iii) Incident to an otherwise permitted use and disclosure
  - (iv) Limited Data set for the purposes of research, public health or health care operations.
  - (v) If individual is informed in advance and has the opportunity to Agree or to Object
  - (vi) For Public Interest and Benefit Activities
- (2) Required: A CE is required to disclose PHI:
  - (i) To individual
  - (ii) To HHS when it is undertaking a compliance investigation
- (3) BA – Permitted: A BA is permitted to use or disclose PHI only as permitted by its BA contract.
- (4) BA – Required: A BA is required to disclose:
  - (i) To HHS to investigate or determine the BA's compliance
  - (ii) To CE or individual
- (5) Prohibited:
  - (i) A health plan shall not use or disclose PHI that is genetic info for underwriting purposes.
  - (ii) A CE/BA may not sell PHI

(b) Standard: Mimimum necessary applies:
- (1) A CE must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

(c) Standard: Uses and Disclosures of PHI subject to an agreed upon restriction:
A CE that has agreed to a restriction may not use or disclose PHI covered by the restriction.

(d) Standard: Uses and Disclosures of de-identified PHI
- (1) A CE may use PHI to create information that is not identifiable or disclose PHI only to a BA for such purpose.
- (2)(i) Disclosure of a code of de-identified information to be re-identified constitutes disclosure of PHI.
  - (ii) If de-identified information is re-identified, A CE may use or disclose such re-identified information.

(e)(1)Standard: Disclosures to BA:
- (i) A CE may disclose PHI to a BA with assurance from BA.
- (ii) A BA may disclose PHI to a BA that is subcontractor with satisfactory assurance.

(f) Standard: A CE must comply for a period of 50 years following the death of individual.

PHI = Protected Health Information, CE = Covered Entity
BA = Business Associate

164.508
Uses & disclosures for which an authorization is required

(a) Std: Authorization for Uses and Disclosures:
- (1) General Rule: (R) A CE may not use or disclose PHI without an authorization.
- (2) Psychotherapy Notes: (R) A CE must obtain an authorization for any use or disclosure of psycho-therapy notes with few exceptions.
- (3) Marketing: (R)
  - (i) A CE must obtain an authorization for any use or disclosure of PHI for marketing,except,
    - (A) A face-to-face communication made by a CE to an individual; or
    - (B) A promotional gift of nominal value provided by the CE.
  - (ii) If the marketing involves financial remuneration to the CE from a third party, the authorization must state that.
- (4) Sale of PHI: (R)
  - (i) A CE must obtain an authorization for any disclosure of PHI which is a sale of PHI.
  - (ii) Such authorization must state that the disclosure will result in remuneration to the CE.

(c) Implementation specifications: Core Elements and Requirements
- (1) A valid authorization must contain core elements.
- (2) In addition to core elements, the authorization must contain required statements (R)
- (3) The authorization must be written in plain language.
- (4) CE must provide copy of signed authorization.

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

(a) Std: Permitted Uses and Disclosures: A CE may use or disclose PHI for treatment,payment,or health care operations.

(b) Std: Consent for uses and disclosures permitted:
- (1) A CE may obtain consent of the individual to use or disclose PHI.
- (2) Consent is not effective if authorization is required.

(c) Implementation specifications:
- (1) A CE may use or disclose PHI for its own treatment, payment, or health care operations.
- (2) A CE may disclose PHI treatment activities of a health care provider.
- (3) A CE may disclose PHI to another CE for payment activities.
- (4) A CE may disclose PHI to another CE for healthcare operation activities.
- (5) A CE that participates in organized healthcare arrangement may disclose PHI to other participants in organized heatlh care.

SubPart-E

(Privacy of Individually Identifiable Health Information)

164.520
Notice of Privacy Practices for PHI

(a) Std: Notice of Privacy Practices:
(1) Right to Notice: Each CE, with certain exceptions for group health plans and Inmates, must provide a notice of its privacy practices.
(b) Implementation specifications: Content of Notice:
(1) Required Elements: Notice
☐ Must be in plain language, including a header.
☐ Must contain a separate statement for certain uses and disclosures.
☐ Must state the CE's duties to protect privacy, and abide by the terms of the current notice.
☐ Must describe Individual's rights, including the right to complain to HHS and to the CE if they believe their privacy rights have been violated.
☐ Must include a point of contact for further information and for making complaints to CE.
☐ Must contain the date on which the notice is first in effect.
(3) Requirements for Electronic Notices:
☐ A CE that maintains a website must prominently post the notice on its website.
☐ A CE must provide notice thru email if individual agrees to electronic notice and the individual retains the right to obtain a paper copy.

164.522
Rights to Request Privacy Protection for PHI

(a) (1) Std: Right of an individual to request restriction of Uses and Disclosures: Individuals have the right to request that a CE restrict use or disclosure of PHI for treatment, payment or healthcare operations.
(b) (1) Std: Confidential Communications Requirements: A covered health care provider and a health plan must permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that the CE typically employs.

164.524
Access of Individuals to PHI

(a) (1) Std: Access to PHI: Individuals have the right to review and obtain a copy of their PHI.

164.526
Amendment of PHI

(a) (1) Std: Right To Amend: Individuals have the right to have CEs amend their PHI in a designated record set when that information is inaccurate or incomplete.
(2) A CE may deny an individual's request for amendment if it determines the PHI was not created by CE, or not part of designated record set or is inaccurate or incomplete.

164.528 - Accounting of Disclosures of PHI

(a) Standard:
(1) An individual has a right to receive an accounting of disclosures of PHI made by a CE in the six years prior to the date on which the accounting is requested.
(2) The CE must temporarily suspend in individual's right to receive an accounting of disclosures to a health oversight agency or official if such agency or official provides the CE with a written statement that such an accounting would impede agency's activities.

164.530 - Administrative Requirements

(a) (1) Standard: Personnel Designations:
(i) A CE must designate a privacy official
(ii) A CE must designate a contact person or office
(2) A CE must document the personnel designations.
(b) (1) Standard: Training: A CE must train all workforce members on its privacy policies and procedures.
(2) A CE must provide training within reasonable period of time and document that the training has been provided.
(c) (1) Standard: Safeguards: A CE must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
(2) A CE must reasonably safeguard PHI from any intentional or unintentional use or disclosure in violation of the Privacy Rule.
(d) (1) Standard: Complaints to the CE: A CE must have procedures for individuals to complain about its compliance with its privacy policies and procedures.
unintentional use or disclosure in violation of the Privacy Rule.
(2) A CE must document all the complaints.
(e) (1) Standard: Sanctions: A CE must have and apply appropriate sanctions against workforce members who fail to comply.
(2) A CE must document the sanctions that are applied.
(f) Standard: Mitigation: A CE must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its workforce or its BA's in violations of its privacy policies and procedures.
(g) Standard: Refraining from Intimidating or Retaliatory Acts: A CE may not retaliate against a person for exercising rights provided by the Privacy Rule.
(h) Standard: Waiver of rights: A CE may not require an individual to waive any right under the Privacy Rule.
(i) (1) Standard: Policies and Procedures: A CE must develop and implement written privacy policies and procedures.
(2) Standard: Changes to policies or procedures: A CE must change its policies and procedures as necessary and appropriate to comply with changes in law.
(j) (1) Standard: Documentation: A CE must maintain policies and procedures in written or electronic form
(2) A CE must retain the documents of its privacy policies and procedures, its privacy practices notices, disposition of complaints, other actions, activities for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

PHI = Protected Health Information, CE = Covered Entity, BA = Business Associate