# HIPAA Administrative Simplification Statute and Revised Rules

**Compliance Deadline: September 23, 2013**

**New York State Chiropractic Association**
777 Lisha Kill Road
Niskayuna, NY 12309-3142
(518) 785-6346
(518) 785-6352 (f)
www.nysca.com
info@nysca.com

The following material and information and any reports relating thereto are the property of the New York State Chiropractic Association (NYSCA). Any errors, typographical, calculable or otherwise found herein are not intentional or intended to mislead. Readers who become aware of any factual errors or errors of content should notify the NYSCA as soon as is reasonably possible so that these may be examined and corrected if necessary. The Association accepts no responsibility for the information reported herein and cannot be held liable for errors of content or omission in this manual. Any and all questions regarding this information should be directed to the NYSCA.



New York State Chiropractic Association
777 Lisha Kill Road
Niskayuna, NY 12309-3142

Table of Contents

[The Page Intentionally Left Blank for Two-Sided Printing]

September 20, 2013

DRAFTED BUT NOT PROOFREAD

Gentlepersons,

As you may or may not know, new and revised Health Insurance Portability and Accountability Act (HIPAA) rules take effect, Monday September 23, 2013. These changes have been prompted by the Health Information Technology for Economic and Clinical Health Act (HITECH) enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5). Although HIPAA is extensive insofar as federal law are concerned, the main portions of HIPAA affecting chiropractic providers are HIPAA's Administrative Simplification provisions – an oxymoron if there ever was one – principally the Privacy and Security Rules and the Breach Notification requirements. In addition, a state may have more stringent requirements that exceed the federal law, in which case the requirements state law must also be addressed; or, alternatively, some states have laws that have few or no stipulations in these topical areas, in which case the federal HIPAA requirements form the baseline that practices must follow.

Most practices should be acquainted with the Privacy and Security rules already, since these provisions have been in place for nearly ten (10) years or more. As you well know, the Privacy Rule restricts the use and disclosure of a patient's or beneficiary's "protected health information" (PHI), if the practice transmits PHI electronically, such as by filing claims or confirming a patient's coverage electronically. The Security Rule, in contrast, required practices to institute a number of safeguards – administrative, technical and physical – to protect the confidentiality as well as the integrity of electronic PHI.

■Good News and Not-so-good News

■Good News

In the previous or earlier version of the HIPAA rules, covered entities that entered into contracts with "business associates" (BA) – e.g., a billing or claims service, electronic medical record software company, or some other health information technology or networking hardware or software vendor[1] – or a subcontractor of a business associate – unduly burdened a practice by making the practice responsible for the activities of the business associate insofar as the HIPAA Privacy and Security Rules were concerned. The Rules also required that a covered entity notify HHS and those affected if the BA breached the HIPAA Rules, inadvertently or otherwise.

The latest modification of the HIPAA Rules lifts the burden on covered entities to some degree by placing the obligation for compliance with the HIPAA Rules squarely onto contracted business associates.[2,3] Consequently, the Rules have been modified throughout to make the individual HIPAA provisions apply to "covered entities or business associate." Furthermore, business associates are responsible for compliance on the part of any BA's subcontractors.[4]

If you already have and have had a contract with a business associate prior to the effective of the revised regulations, January 25, 2013 and the contract comports with the previous HIPAA regulations and has not been modified or amended between March 26,2013 and September 23, 2013, the contract is still valid and

need not be modified until September 22, 2014 at the very latest.[5] If, however, the practice has signed a new agreement post January 25, 2013 or modified or amended a pre-existing business associate contract between March 26, 2013 and the September 23, 2013 compliance date, the contract must comply with the revised HIPAA provisions by September 23, 2013.[6]

■Not So Good News

There are parts and provisions in the revised HIPAA Rules that do apply to providers.

Providers should be aware that some of the definitions in the Security Rule have changed. The definition of *administrative safeguards* and *physical safeguards* were revised respectively to read as follows:

> *Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.[7]
>
> *Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.[8]

Like the previous version of the HIPAA Rules, some of the new and revised measures are "Required" which means that a covered entity or business associate "*must implement*" the stipulated measure[9]; others are "Addressable" meaning that the covered entity or business associate must assess and determine whether each implementation specification is a *reasonable and appropriate safeguard* in its environment.[10] Further, a practice or business associate "*must review and modify* the security measures implemented" . . . to continue the provision of reasonable and appropriate protection as needed and to update the documentation relevant to the measures adopted.[11]

In accord with the revised Security Rule, covered entities and business associates are "Required" to conduct a *Risk Analysis* to assess the "potential risks and vulnerabilities to the confidentiality, integrity, and availability" of electronic PHI.[12] Covered entities and business associates are also "Required" to have and maintain a *Sanction policy* to apply against members of the workforce "who fail to comply with the security policies and procedures of the office/practice.[13] The Rule was also modified to require that a covered entity "[i]dentify and respond to suspected or known security incidents"; to document the incident and mitigate where possible any harmful effects stemming from the incident.[14]

Addressable standards included a *Termination procedure* the implements a process for terminating or otherwise ending access to PHI when a workforce member's employment ends.[15] In a similar manner, a practice must provide an *Access establishment and modification* policy and procedure that address when, where and how a user may access a workstation, transaction, program or process.[16]

In addition, revisions were made to the Administrative Safeguards requiring a practice or business association to identify a security official responsible for development and implementation of the required or addressable policies and procedures.[17]

■Breach in the confidentiality and safeguarding of confidential protected health information.

The portion of the HIPAA regulations related to a breach – some failure to maintain or secure PHI was modified at § 164.402 to read as follows:

> **§ 164.402 Definitions.**
> As used in this subpart, the following terms have the following meanings: *Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.
>
> (1) Breach excludes:
>
> (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
>
> (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
>
> (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
>
> (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
>
> (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
>
> (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
>
> (iii) Whether the protected health information was actually acquired or viewed; and
>
> (iv) The extent to which the risk to the protected health information has been mitigated.

Following the discovery of a breach of unsecured PHI that involves more than 500 residents in one or more jurisdictions, a covered entity is required to "notify prominent media outlets in the state or jurisdiction" without unreasonable delay and, in no case, more than sixty (60) days after discovery of the breach.[18] For breaches

of PHI involving less than 500 individuals, the covered entity "must maintain a log or other documentation of the breach(es) and notify the Secretary/HSS not later than 60 days after the end of each calendar year.[19] In addition, as before, covered entities are required to notify the involved individuals of a breach under § 164.404. That has not changed. If a breach is discovered by a contracted business associate, the business associate must apprise the covered entity of the breach "as of the first day on which [the] beach is known to the business associate.[20]

■Changes to the General Rules for the use and disclosure of Protected Health Information

As doctors will recall, covered entities and business associates "may not use or disclose" a patient's PHI except as permitted or required to the involved individual,[21] for treatment, payment or health care operations,[22] or incident to a use or disclosure otherwise permitted or required by HIPAA,[23] of pursuant to a valid authorization[24] or agreement,[25] or as permitted by and in compliance with other sections of HIPAA.[26]

- **Providing PHI to the an individual in electronic form**
  One significant change as a result of the new rule – a covered entity is "required" to disclose PHI to the involved individual "when requested under, and required by § 164.524 or § 164.528." What is the significance of these two sections? Paragraph (c)(2)(i) of § 164.524 was modified, paragraph (c)(2)(ii) was renumbered (c)(2)(iii) and a new paragraph (c)(2)(ii) was added that requires a covered entity to provide an individual with a copy of her PHI ***in electronic form***, in the form and format requested by individual, if possible, and if not available in the requested form, then in an ***electronic form and format*** mutually agreed upon by the practice and the individual.[27]

  Section 164.528 gives a patient the right to receive an "accounting of such disclosures."

A business associate may also disclose PHI under § 164.502 but only to the Secretary of HHS[28] as required or to a covered entity pursuant to its contract or other arrangement with the covered entity,[29] to the covered entity, the involved individual or the individual's designee.[30]

Section 164.502(e)(1) allows a covered entity to disclose PHI to a business associate or allows the BA to create PHI "to create, receive, maintain and transmit" PHI on the covered entity's behalf, provided the practice obtains satisfactory assurances that the BA will protect and safeguard the information.[31] If the business associate subcontracts, it is the responsibility of the BA to obtain the same assurances from the subcontractor.[32]

In all cases, each must make a "reasonable effort" to limit the disclosure of PHI to "the minimum necessary to accomplish the intended purpose of the use, disclosure or request."[33]

■Organizational requirements

Modifications to § 164.504 are the requirements that apply to contracts with business associates. It will hold a covered entity in non-compliance if the covered entity "knew of a pattern of activity or practice of the business associate" or a subcontractor of the BA, "that constituted a material breach or violation" of either the BA or subcontractor, unless the covered entity took reasonable steps to cure the breach or end the violation.[34]

If your practice has any business associate contracts, you will want to make sure the contracts comport with this section of the Privacy Rule in particular, by the dates and deadlines outlined elsewhere above. As such, you will want to pay particular attention to all of the changes required as outlined in Endnote 34.

■Authorizations

There appeared to be minor changes to § 164.508 dealing with authorizations, except that a new paragraph was added that stipulated that a covered entity must obtain an authorization to sell an individual's PHI and the authorization must state that the covered entity will be remunerated for the disclosure.[35] Compound authorizations – an authorization that covers more than one specific situation, continue to be prohibited generally,[36] but exceptions were made for certain research study purposes[37] and certain stipulations relating to psychotherapy notes.[38] A covered entity may not condition the provision of any treatment, payment, enrollment in a health plan, or eligibility for benefits under a plan on the stipulation that the individual provide an authorization of one sort or another.[39]

■Uses and disclosures requiring an opportunity for the individual to agree or object.

There were modest clarifying revisions changes to portions of § 164.510. The most significant change was the addition of a new paragraph that permits disclosure of an individual's PHI if they are deceased to a family member, other relative, or a close personal friend of the deceased, if they were involved in the individual's care and payment prior to her death and the information is relevant to such person's involvement.[40]

■Uses and disclosures for which an authorization is not required, nor an opportunity to agree or object.

As doctors may recall, this section permits certain uses and disclosures without an authorization and does not provide an opportunity for the individual to either agree or object. As doctors will also recall, some of instances are where the information is required by a court order, for state and federal public health activities, for state workers' compensation programs, to report instances of abuse and neglect where required by state law, and so on. A new paragraph was added to the public health activities subsection (b) that permits disclosure of PHI information limited to proof of immunization to a school as required by state or other law prior to admitting the individual to school.[41] Although the opportunity to agree or object, is not technically required, nonetheless, a covered entity is required to obtain and document the agreement to this particular disclosure from a parent or guardian for an unemancipated minor or from the individual if she is an adult or emancipated minor.[42]

■Notice of Privacy Practices

Modest clarifying revisions have been made to select portions of § 164.520 of the Privacy Rule dealing with the Notice of Privacy Practices. Subsection (b), paragraph (1)(v)(A) reinforces the fact that a covered entity is required to "notify affected individuals following a breach of unsecured protected health information."[43] The only addition in the revised rule was directed at health plans, not providers.[44]

■Right to request privacy protection from protected health information

Again, the revised rule makes some modest clarifying changes to § 164.522 of the privacy rule. Of note to

providers, however, is the addition of subparagraph (vi) to paragraph (1) of subsection (b) of § 164.522. Subparagraph (vi) is important, however, in that it requires that a covered entity agree to an individual's request to restrict disclosure of her PHI, if the disclosure "is for the purpose of carrying out payment or health care operations and is **NOT** otherwise required by law **and** the PHI "pertains solely to a health care item or service for which the individual or person other than the health plan on behalf of the individual, *has paid the covered entity in full* already.[45]

> **§ 164.522 Rights to request privacy protection for protected health information.**
> (a) (1) * * *
> * * * * *
>
> (vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:
> (A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
> (B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

Any restrictions on the use or disclosure of PHI by a covered entity, must be documented.[46]

■Access of Individuals to their PHI

As noted elsewhere above, covered entities "must provide" the individual with access to her PHI in the form and format requested by the individual, if possible, and if not then in a "readable, hard copy form and format to which both mutually agree.[47] This also includes access by the individual to her PHI sent to her in "electronic form."[48] Access must be provided in a "timely manner"[49] and the individual may designate in writing to have another individual to receive the PHI and the covered entity must transmit or provide a copy of the information to the designated person.[50] A covered entity may charge the individual reasonable costs for labor and supplies whether the information is supplied in hard copy/paper form, or electronically.[51]

■Deadline for compliance

The compliance date for the revised HIPAA rule was January 25, 2013 with a drop dead date for compliance is 180 days out from January 25 or September 23, 2103.[52]

■Obligation to Cooperate

Be aware that covered entities and business associates are obliged to keep such records as required by HIPAA, provide such records and compliance reports to the Secretary of HHS, to cooperate with complaint investigations and compliance reviews, and to permit access to the Secretary to its facilities, books, records, accounts and other sources of information, including PHI, that are pertinent to the Secretary's determination of compliance on the part of the entity or business associate.[53] In response to a complaint,[54] the Secretary is obliged to conduct a compliance review "when a preliminary review of the facts indicates a possible violation due to willful neglect."[55] Otherwise, the Secretary may conduct a compliance review "in any other circumstance."[56]

■Audits

Be aware as well that the HITECH Act also requires HHS to perform periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. HHS Office for Civil Rights (OCR) enforces these rules, and in 2011, OCR established an audit program to assess the controls and processes covered entities have implemented to comply with the Rules.[57] The OCR audit protocol contains 169 audit protocols – 78 Security, 81 Privacy and 10 Breach protocols in the following three (3) domains[58]:

1• Privacy Rule requirements for
   (1) Notice of privacy practices for PHI
   (2) Rights to request privacy protection for PHI
   (3) Access of individuals to PHI
   (4) Administrative requirements
   (5) Uses and disclosures of PHI
   (6) Amendment of PHI, and
   (7) Accounting of disclosures.

2• The protocol covers Security Rule requirements for administrative, physical, and technical safeguards

3• The protocol covers requirements for the Breach Notification Rule.

■Violations and Neglect

Although § 160.312 gives the Secretary of HHS the latitude of resolving a HIPAA complaint[59] or an instance of noncompliance upon a review[60] by informal means or measures – e.g., a corrective action plan or other agreement,[61] nonetheless, the HITECH Act upped the compliance ante by requiring that the Secretary impose a "civil money penalty" upon a covered entity or business associate, if the Secretary determines that a violation of a provision of the Administrative Simplification portion of HIPAA has occurred.[62] The Rules create a tiered civil penalty structure for HIPAA violations, ignorance and willful neglect.

| HIPAA Violation[63] | Penalty Range | Annual Maximum |
|---|---|---|
| For a violation in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated such provision[64] | $100 - $50,000 for each violation[65] | $1,500,000 for identical violations during a calendar year[66] |
| For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect[67] | $1,000 - $50,000 for each violation[68] | $1,500,000 for identical violations during a calendar year[69] |

| HIPAA Violation[63] | Penalty Range | Annual Maximum |
|---|---|---|
| For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred[70] | $10,000 - $50,000 for each violation[71] | $1,500,000 for identical violations during a calendar year[72] |
| For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred[73] | $50,000 for each violation[74] | $1,500,000 for identical violations during a calendar year[75] |

In assessing the foregoing penalties, the may consider the following five factors in brief, "which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation;
(b) The nature and extent of the harm resulting from the violation;
(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate;
(d) The financial condition of the covered entity or business associate; and
(e) Such other matters as justice may require.[76]

■Checklist

While not a complete list, the AMA provides a useful HIPAA checklist that you can use to evaluate your current office practices. (See: http://www.ama-assn.org//resources/doc/washington/hipaa-toolkit.pdf)

■Notice of Privacy Practices (Reprise)

In addition to the AMA Guide above, the U.S. Department of Health and Human Services provides "model notices" that doctors can use to tailor the Notice of Privacy Practices you use to fit the circumstances of your personal practice.

See: http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

NPP Provider Files -

NPP Booklet - HC Provider http://www.hhs.gov/ocr/privacy/hipaa/npp_booklet_hc_provider.pdf
NPP Layered - HC Provider http://www.hhs.gov/ocr/privacy/hipaa/npp_layered_hc_provider.pdf
NPP Full Page - HC Provider http://www.hhs.gov/ocr/privacy/hipaa/npp_fullpage_hc_provider.pdf
NPP HC Provider - Text Version http://www.hhs.gov/ocr/privacy/hipaa/npp_hc_provider-text_version.doc

■Complete Regulations are attached

The complete regulations, including all of the updates to the HIPAA Privacy and Security Rules are attached below. If you have any questions about any particular aspect of either the HIPAA Privacy or Security Rule, please let me know.

References

1. 45 CFR 160.103 Definitions – Business Associate

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:
   (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 45 CFR 3.20, billing, benefit management, practice management, and repricing; or
   (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:
   (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
   (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.
   (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does NOT include:
   (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
   (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.
   (iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
   (iv) A covered entity participating in an organized health care arrangement that

performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

2. 45 CFR 164.308 – Administrative safeguards

(b) (1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

3. 45 CFR 164.314 – Organizational requirements

**§ 164.314 Organizational requirements.**

(a) (1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required).*

(i) *Business associate contracts.* The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

4. 45 CFR 308 – Administrative safeguards (b):

> (b) (1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
>
> (2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.
>
> (3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

5. 45 CFR 164.532 – Transition Provisions, (e) – Qualification

6. 45 CFR 164.532 – Transition Provisions, (e) – Qualification

7. 45 CFR 164.304 – Definitions, *Administrative safeguards*. See also: http://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-304.pdf

8. 45 CFR 164.304 – Definitions, *Physical Safeguards*.

9. 45 CFR 164.306 – Security standards: General, (d)(2).

10. 45 CFR 164.306 (d)(3)

11. 45 CFR 164.306(e).

12. 45 CFR 164.308 – Administrative safeguards, (a)(1)(ii)(A).

> (a) A covered entity or business associate must, in accordance with § 164.306:
>
> (1) * * *
>
> (ii) * * *
>
> (A) *Risk analysis (Required).* 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 or business associate.

13. 45 CFR 164.308 (a)(1)(ii)(C).

> (a) A covered entity or business associate must, in accordance with § 164.306:

(1) * * *

(ii) * * *

* * * * *

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

14. 45 CFR 164.308 (a)(6)(ii).

(a) A covered entity or business associate must, in accordance with § 164.306:

(6) * * *

(ii) *Implementation specification: Response and reporting (Required).* 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 or business associate; and document security incidents and their outcomes.

15. 45 CFR 164.308 (a)(3)(ii)(C).

(a) A covered entity or business associate must, in accordance with § 164.306:

(3) * * *

(ii) * * *

(C) *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

16. 45 CFR 164.308 (a)(4)(ii)(C).

(a) A covered entity or business associate must, in accordance with § 164.306:

(4) * * *

(ii) * * *

(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

17. 45 CFR 164.308 (a)(2).

18. 45 CFR 164.406– Notification to the media, (a),(b).

19. 45 CFR 164.408 (c).

20. 45 CFR 164.410 – Notification by a business associate.

(a) *Standard*

(1) *General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

* * * * *

21. 45 CFR 164.502 – Uses and disclosures of protected health information: General rules, (a) standard, (1)(i).

22. 45 CFR 164.502(a)(1)(ii) as permitted by and in compliance with § 164.506.

23. 45 CFR 164.506 (a)(1)(iii) provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure.

24. 45 CFR 164.502 (a)(1)(iv) pursuant to and in compliance with a valid authorization under § 164.508.

25. 45 CFR 164.502 (a)(1)(v) as permitted by § 164.510.

26. 45 CFR 164.502 (a)(1)(vi) and sections § 164.512, § 164.514(e), (f), or (g).

27. 45 CFR 164.524 (c)(2)(i), (ii):

(c) * * *

(2) *Form of access requested.*

(i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity **must provide** the individual with access to the protected health information **in the electronic form and format requested by the individual**, if it is readily producible in such form and format; or, *if not*, **in a readable electronic form and format as agreed to by the covered entity and the individual**. (Emphases, italics and underlining added.)

28. 45 CFR 164.502 (a)(3) and (a)(4)(i).

29. 45 CFR 164.502 (a)(3) and (a)(4)(ii).

30. 45 CFR 164.502 (a)(4)(ii).

31. 45 CFR 164.502 (e)(1)(i).

32. 45 CFR 164.502 (e)(1)(ii).

33. 45 CFR 164.502(b)(1).

34. 45 CFR 164.504 (e)(1)-(3) and (f).

(e) (1) Standard: Business associate contracts.
(i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.
(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.
(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.
(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:
(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:
(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and (B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
(ii) Provide that the business associate will:
(A) Not use or further disclose the information other than as permitted or

required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) Implementation specifications: Other arrangements.

(i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of

paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.

(4) Implementation specifications: Other requirements for contracts and other arrangements.

(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B) (*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which

it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f) (1) * * *

(ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

* * * * *

(2) * * *

(ii) * * *

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

* * * * *

35. 45 CFR 164.508(a)(4)(i).

36. 45 CFR 164.508 (b)(3).

37. 45 CFR 164.508 (b)(3)(i).

38. 45 CFR 164.508 (b)(3)(ii).

39. 45 CFR 164.508 (b)(3)(iii).

40. 45 CFR 164.510 – Uses and disclosures requiring an opportunity for the individual to agree or to object, (b)(1) and (b)(5).

41. 45 CFR 164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required, (b) Standard: Uses and disclosures for public health activities, (vi).

42. 45 CFR 164.512 (b)(vi)(C)(1) and (2).

43. 45 CFR 164.520 Notice of privacy practices for protected health information, (b)(1)(v)(A).

44. 45 CFR 164.520 (c)(1)(v)(A) and (B).

45. 45 CFR 164.522 – Rights to request privacy protection for protected health information, (a)(1)(vi).

46. 45 CFR 164.522 (a)(3).

47. 45 CFR 164.524 – Access of individuals to protected health information, (c)(2) – Form of Access requested, (i).

48. 45 CFR 164.524 (c)(2)(ii) as follows:

> **§ 164.524 Access of individuals to protected health information.**
> (c) * * *
> (2) *Form of access requested.*
> (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.
> (ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.
> * * * * *

49. 45 CFR 164.524 (c)(3)(i).

50. 45 CFR 164.524 (c)(3)(ii).

51. 45 CFR 164.524 (c)(4).

52. 45 CFR 160.105 – Compliance dates for implementation of new or modified standards and implementation specifications.

53. 45 CFR 160.310 – Responsibilities of covered entities and business associates

54. 45 CFR 160.306 – Complaints to the Secretary.

55. 45 CFR 160.308 – Compliance reviews, (a).

56. 45 CFR 160.308(b).

57. See: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

58. See: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

59. 45 CFR 160.306 – Complaints to the Secretary

60. 45 CFR 160.308 – Compliance reviews

61. 45 CFR 160.312 – Secretarial action regarding complaints and compliance reviews.

62. 45 CFR 160.402 – Basis for a civil money penalty.

63. 45 CFR 160.404 – Amount of a civil money penalty. See also: http://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec160-404.pdf

64. 45 CFR 160.404 - Amount of a civil money penalty, (b)(2)(i).

65. 45 CFR 160.404 (b)(2)(i)(A).

66. 45 CFR 160.404 (b)(2)(i)(B).

67. 45 CFR 160.404 (b)(2)(ii)

68. 45 CFR 160.404 (b)(2)(ii)(A)

69. 45 CFR 160.404 (b)(2)(ii)(B)

70. 45 CFR 160.404 (b)(2)(iii)

71. 45 CFR 160.404 (b)(2)(iii)(A)

72. 45 CFR 160.404 (b)(2)(iii)(B)

73. 45 CFR 160.404 (b)(2)(iv)

74. 45 CFR 160.404 (b)(2)(iv)(A)

75. 45 CFR 160.404 (b)(2)(iv)(B)

76. 45 CFR 160.408 – Factors considered in determining the amount of a civil money penalty.

    In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

    (a) The nature and extent of the violation, consideration of which may include but is not limited to:
        (1) The number of individuals affected; and
        (2) The time period during which the violation occurred;
    (b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:
        (1) Whether the violation caused physical harm;
        (2) Whether the violation resulted in financial harm;
        (3) Whether the violation resulted in harm to an individual's reputation; and
        (4) Whether the violation hindered an individual's ability to obtain health care;
    (c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:
        (1) Whether the current violation is the same or similar to previous indications of noncompliance;
        (2) Whether and to what extent the covered entity or business associate has

attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

**5691 Federal Register** / Vol. 78, No. 17 / Friday, January 25, 2013 / Rules and Regulations