HIPAA Compliance

Investigations & Penalties

Prepared by Kenneth E. Rhea, MD, FASHRM

Brought to you by

DUXWARE™

...LEADING THE WAY IN TECHNOLOGY FOR HEALTHCARE PROVIDERS

www.duxware.com

The Event

In December 2014 an internal medicine practice employee placed an Ultrabook computer in her personal car. The computer contained the data and conclusions of a recent study of practice patients with cardiac pathology. The information included patient names, office file numbers, patient final diagnosis, insurance information, and current treatment plans. The study had involved 275 patients over a two year period. The practice employee s car was stolen on a Friday evening including the Ultrabook computer. Report of the theft and loss of the patient information was not done until the next Wednesday after the employee conducted a search for the vehicle which was never found. It was determined by the practice that a report and notifications should be made, however the practice, though having appointed a Privacy Officer in the past three years prior, had no policies or mechanisms in place for necessary actions. Another employee reported the incident to the office of the Secretary of HHS. Are potential liability problems present?

Investigation & Penalties

Brief History

With a stated general purpose to make certain other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities the government published January 25, 2013 through the Office for Civil Rights a new and extensive set of regulations.[1] This Rule, now the most recent regulation with a compliance date of September 23, 2013, includes significant modifications to parts of other earlier rules and also adopts interim rules already in place.[2] The official name of the new set of regulations was:

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

For ease of discussion it has become known with the shorter name of the Omnibus Final Rule (OFR) or Megarule and was in itself composed of four rules one of which was to finalize modifications issued as a proposed rule on July 14, 2010.[3] One of

"If it appears that the violation possibly involves □willful neglect□ an investigation □will□be done."

the four rules has several parts a section of which relates to access of protected health information (PHI). The purpose of this article is to discuss the now currently modified regulations relating to compliance, investigations, and penalties.

Under HIPAA Administrative Simplification Regulations (□160.306) a person has the right to complain directly to the Secretary of HHS.[4] Certain requirements are present, e.g. a complaint must be filed in writing and can also be filed electronically. The complaint must be filed within 180 days of when the person making the complaint knew or should have known about the act and it must □ □ name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s)." [5]

When such a complaint is made an initial evaluation of the provided information (□ preliminary review□) will be made.[6] If the information comes to the attention of the HHS through a federal or state agency a compliance review rather than an investigation might be made.[7] If it appears that the violation possibly involves □ willful neglect□ an investigation □ will□ be done.[8] The OFR currently defines □ willful neglect□ as □ □ conscious, intentional failure or reckless indifference to the obligation to comply with the administrative

"the covered entity (CE) in question would be contacted by OCR with a description of the alleged acts of non-compliance"

simplification provision violated.[9] The OFR discusses the consideration of probable, but determines that all possible situations will be investigated and that probable is not a consideration. However, the new OFR is clear in confirming that HHS has the discretion to decide whether or not after a preliminary review a compliance review or a complaint investigation will be done.[10] In prior Administrative Simplification regulations OCR was given discretion to investigate complaints through the use of may. Under the OFR in order to incorporate the provisions of HITECH Act 13401(a) a new section (160.306 (c)(1)) has been added making clear that the Secretary will investigate complaints in which the preliminary review indicates a possible violation due to willful neglect, though there is continued discretion of investigation for any other complaints.[11]

In a usual situation the covered entity (CE) in question would be contacted by OCR with a description of the alleged acts of non-compliance.[12] Notwithstanding the reason for the investigation the investigation may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.[13]

Additionally it is necessary for the covered entity (CE) or business associate (BA) to keep such

"it is essential for the covered entity or business associate to be prepared for and to have the intent to ooperate with the OCR"

records in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions".[14] This represents a critical reason for all covered entities to have well organized systems including policies, procedures, and tracking mechanisms.

It is essential for the covered entity or business associate to be prepared for and to have the intent to cooperate with the OCR when a compliance review or investigation is taking place. Such cooperation includes allowing access during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions.[15] If the information needed for the compliance review or investigation is not available to the covered entity (CE), e.g. held by some other entity, there must be a formal certification of that fact and a description of the efforts made to obtain the information.[16] It should also be noted that if it is felt by the OCR in the course of the compliance review or investigation that exigent circumstances exist , e.g. documents were hidden or destroyed, there will be no restriction on

"...though a preliminary review may not have indicated willful neglect the OCR has the authority to continue to make such a determination as the evidence is obtained and reviewed"

when the investigators may access without notice the areas being investigated.[17] Even though a preliminary review may not have indicated willful neglect the OCR has the authority to continue to make such a determination as the evidence is obtained and reviewed.[18] When the OCR is conducting a compliance review or investigation the regulations provide that any protected health information (PHI) involved will not be disclosed except as necessary in □ □ ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C.552a(b)(7).□ [19] This Privacy Act section (5 U.S.C.552a(b)(7)) permits the □ □ disclosure of a record on an individual contained within a government system of records protected under the Privacy Act to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law and if the agency has made a written request to the agency that maintains the record.□ [20] By this change in the OFR it has been stated that more cooperation is allowed with other law enforcement agencies, e.g. State Attorneys General in the enforcement of state civil actions related to HIPAA. The OFR explains that the OCR in the course of compliance reviews and investigations will be working with not only enforcement agencies,

"The HITCH Section 13410(d) specifically revised the Section 1176(a) of the Social Security Act to establish four categories of violations... "

e.g. State Attorneys General, but also agencies such as the Federal Trade Commission (FTC) in □ □ violations that implicate both HIPAA and the FTC Act.□ [21]

Regulatory Penalties

The HIPAA Enforcement Rule applies to all of the HIPAA Administrative Simplification Rules, as well as the Breach Notification Rule.[22] When the HITECH Act, as part of ARRA, was passed Section 13410 of the Act made amendments to the Social Security Act for the stated purpose of strengthening the HIPAA Enforcement Rule. On October 30, 2009 HHS issued an Interim Final Rule (IFR) which revised the Enforcement Rule and incorporated provisions of HITECH Section 13410(d). This change was to take effect immediately for violations of HIPAA occurring after the enactment date, i.e. February 18, 2009. [23] The HITECH Section 13410(d) specifically revised the Section 1176(a) of the Social Security Act to establish four categories of violations that □ reflect increasing levels of culpability□ relating to □ four corresponding tiers of penalty amounts□ "[24] These new penalty amounts increased the minimum penalty for each violation, with □ a maximum penalty amount of $1.5 million annually for all violations of an identical provision.□ [25] This represented a significant increase in penalty levels.

" "reasonable cause," "reasonable diligence," and "willful neglect."

Section 1176(b) of the Social Security Act was also amended by HITECH Section 13410(d) in removal of the past □ □ affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation.□ [26] This type of violation is now punishable in the lowest tier of penalties. Along with this penalty increase the amendment also included a □ prohibition on the imposition of penalties for any violation that is timely corrected, as long as the violation was not due to willful neglect.□ [27]

In the past CFR □160.410 contained the definitions of several terms used by the HITECH Act Section 13410(d) to describe □ □ increasing levels of culpability□ □ for which corresponding penalties may be imposed.[28] These terms were "reasonable cause," "reasonable diligence," and "willful neglect."[29] In the OFR these definitions have been moved to CFR □160.401. While the latter two definitions were not changed there was modification to □ reasonable cause□ .[30]

As noted above the HITECH Act revised Section 1176(a) of the Social Security Act to establish four tiers of increasing penalty amounts. These tiers would correspond to the □ □ levels of culpability□ □ in the violation.[31]

Penalty Levels [32]

"HHS feels that the □state of mind□or □mens rea□has clarity for the first, third, and fourth levels, but not the second or □reasonable cause□"

1. The first level (least penalty tier) was the new level in which □ □ the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of a violation.□

2. The second level (next highest penalty tier) was that which applied to violations due to reasonable cause and not to willful neglect.

3. The third level was that which applied to situations in which violation was due to willful neglect, but was corrected □ □ within a certain time period□ (30 days).

4. The fourth level was that which applied to the same situations as level 3, but the willful neglect was not corrected.

HHS feels that the □ state of mind□ or □ mens rea□ has clarity for the first, third, and fourth levels, but not the second or □ reasonable cause□ . [33]
The change in definition in □160.401 was intended to address the □ state of mind□ question. The definition of □ reasonable cause□ currently is shown as,
□ Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would

"HHS is represented as working with State Attorneys General to coordinate enforcement "

have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. [34]

Initially under the HITECH Act the Subtitle D provisions were effective one year after the Act enactment, i.e. February 18, 2010 unless other dates were specified. There are some exceptions to this time period, e.g. the tiered and increased civil money penalties of Section 13410(d) referenced above were to affect violations immediately after the date of enactment.[35] Another example is Section 13410(a)(1) which discusses a barring of the Secretary of HHS to impose a civil money penalty (CMP) when a criminal penalty has been imposed. This provision became effective on or after February 18, 2011.[36] The OFR adopts prior amendments to the HITECH Act and explains that HHS will coordinate with the Department of Justice (DOJ) in the referring of cases which might involve criminal HIPAA violations. Also HHS is represented as working with State Attorneys General to coordinate enforcement in compliance with HITECH Section 13410(e).[37] It should also be noted that HITECH Section 13404(c) applies both the civil and criminal penalties to business associates (BA).[38] The OFR states that the the risk of criminal and/or civil monetary penalties may spur some business associates to increase their

efforts to comply with the Rules". [39]

"covered entities (CE) or others covered under the regulations that knowingly obtained or disclosed individually identifiable health information in violation of the regulations were liable for monetary fines and up to one year in prison."

The HIPAA Administrative Text while addressing Civil Money Penalties (CMP) in Subpart D §160.400 to §160.426 does not outline detail on criminal penalties.[40] However, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (HIPAA) criminal enforcement is addressed in 42 U.S.C. §1320d-6.[41]

Since the publication of the initial Rules, there had been some expressed concerns of HHS about the scope of the enforcement provisions and who might be held criminally liable. These concerns were addressed by the Department of Justice (DOJ) in communication to the General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on June 1, 2005.[42] There were two conclusions. One determination was that covered entities (CE) or others covered under the regulations that knowingly obtained or disclosed individually identifiable health information in violation of the regulations were liable for monetary fines and up to one year in prison. If the information was obtained under false pretenses the liability could involve monetary fines and up to five years imprisonment. If there was intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm there could be

"individuals within an organization, e.g. directors, officers, or employees where the covered entity (CE) is not an individual may also be criminally liable under HIPAA. "

fines and up to ten years imprisonment.[43] The second determination was that knowingly was interpreted as requiring only knowledge of the actions that constituted the violation. Specific knowledge of the action being in violation of a HIPAA regulation was not necessary. [44] It was also pointed out that individuals within an organization, e.g. directors, officers, or employees where the covered entity (CE) is not an individual may also be criminally liable under HIPAA. Even in situations where an individual within a covered entity (CE) is not liable under HIPAA they might be charged with conspiracy or aiding and abetting.[45]

Event Review

The practice should have done past risk reviews related to the Privacy Rule, the later Security Rule, the HITECH Act under ARRA, and most recently the Omnibus Final Rule (OFR). The review should have allowed the implementation of appropriate policies, but none were present. It is very probable that a preliminary investigation will occur due to the report to HHS and that the initial investigation will reveal evidence of possible willful neglect which will require the OCR to investigate. The full investigation would show the complete absence of satisfactory effort and appropriate policies. If such findings are present in the required investigation it is probable that a liability determination will be made resulting

in a civil fine. While not absolute it is unlikely that the violation knowingly occurred or was intended and therefore there would not be referral for criminal action. However, it is also probably that willful neglect was present and that the liability could be significant resulting in a significant civil fine and entrance into a Resolution Agreement (RA) and Corrective Action Plan (CAP) with the OCR.

Conclusion

Again the information shown above clearly indicates that the new regulations relating to investigations and penalties have changed in many respects. Many of the elements of earlier regulations, e.g. Privacy Rule, Security Rule, and the HITECH Act have been continued while many have been modified. In order to remain compliant with these regulations and avoid potential liability it is important to review all of the relevant areas with particular attention to the modifications allowing incorporation of current requirements in risk reviews, policies, implementation processes, and tracking procedures.

Questions and Answers after the Endnotes section.

(Endnotes)

1 Federal Register. Omnibus Final Rule. Government Printing Office.gov. Executive Summary and Background. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5566

2 ibid

3 Federal Register. Omnibus Final Rule. Government Printing Office.gov. Executive Summary and Background. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17

4 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.20

5 Ibid p.20. (b)(2)

6 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf Published 1/25/2013. Vol.78; No.17;p5579

7 Ibid

8 Ibid p.5578

9 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.20

10 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5579

11 Ibid p.5578

12 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.20

13 Ibid

14 Ibid

15 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.21

16 Ibid

17 Ibid

18 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5579

19 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.21

20 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5579

21 Ibid

22 Ibid p.5577

23 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5577

24 Ibid

25 Ibid

26 Ibid

27 Ibid

28 Ibid p. 5579

29 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.23

30 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5580

31 Ibid

32 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.24

33 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5580

34 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.

gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.23
35 Federal Register. Omnibus Final Rule. Government Printing Office.gov. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5569
36 Ibid
37 Ibid
38 Ibid p.5597
39 Ibid p.5677
40 US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013. p.10
41 Health Insurance Portability and Accountability Act of 1996. Public law 104-191. Site: www.gop.gov. http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf. Pub. 1996. Accessed March 10, 2014
42 Department of Justice. Scope of Criminal Enforcement Under 42 U.S.C. §1320d-6. Site: www.justice.gov. http://www.justice.gov/olc/opinion/scope-criminal-enforcement-under-42-usc-1320d-6. Pub. June 1, 2005. Accessed March 10, 2014
43 Ibid
44 AMA, HIPAA Violations and Enforcement. Site:www.ama-assn.org. http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page. Accessed March 8, 2014
45 Department of Justice. Scope of Criminal Enforcement Under 42 U.S.C. §1320d-6. Site: www.justice.gov. http://www.justice.gov/olc/opinion/scope-criminal-enforcement-under-42-usc-1320d-6. Pub. June 1, 2005. Accessed March 10, 2014

Review Questions

Question 1 A past employee of a medical practice felt that he had observed a clear violation of the HIPAA Security Rules while he was employed. After he had obtained employment at another medical facility 7 months later he decided to report the violation to the Secretary of HHS. Will the reported violation be a problem to the medical practice?

1. The employee has every right to report the violation and under current regulations since the individual actually worked within the medical practice the violation will be investigated.

2. To receive attention from HHS the presumed violation must be reported to the Secretary of HHS within a reasonable period of time to be

determined by HHS after receiving the report.

3. The presumed violation must be reported no sooner than 6 months providing time for the reporting person to gather all possible information, e.g. names, dates, etc. to accompany the report.

4. A report must be filed within 180 days of when the person reporting the alleged violation knew or should have known of the violation.

Answer: 4

The reporting time is specific being related to when knowledge of a possible violation has occurred, i.e. "...when the person making the complaint knew or should have known about the act...". There is no judgement of "reasonable time".

Question 2 A medical practice administrator had determined with the approval of practce owners tht the implementation of certain parts of the Privacy Rule was putting an undue burden on the medical practice. These areas were therefore not addressed on policies and were not included in education of medical supervision or staff. In relation to one of the privacy areas not addressed a complaint was filed to the Secretary of HHS in writing by an employee. The complaint concerned what was perpceived to be a violation of the Privacy Rule and was made 40 days after the employee knew of the violation.

1. An initial preliminary review will be made and since it appears that the failure to follow the regulations was deliberate "willful neglect" a following investigation must be made by the Office for Civil Rights (OCR).

2. The employee cannot make such a complaint to the Secretary of HHS since whether or not policies existed the employee had an obligation to correct the privacy concerns.

3. An initial preliminary review connot possibly determine the possibility of willful neglect and it is within the discretion of the Office for Civil Rights (OCR) to determine whether or not any further action will be taken.

4. There was not a complete absence of medical supervisors and staff on HIPAA regulations, therefore it must be assumed that there was intent to provide privacy and security of protected health information (PHI) removing the possibility of a willful neglect determination.

Answer: 1

"Willful neglect" is defined as "...conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." When the initial preliminary review of a complaint indicates that willful neglect might be "possible" there is an

Kenneth E. Rhea, MD, FASHM

Dr. Rhea is a medical liability and risk consultant to medical practices and other health related organizations. He was in medical and surgical practice for over 30 years and for the past 17 years has been a consultant in medical risk and liability management. He is the owner and Managing Partner of Medical Education and Risk Consulting, called MER Consulting. Dr. Rhea has been dealing with risk and federal regulatory compliance areas such as the HIPAA privacy and security regulations beginning with the Privacy Rule in 2000.

Dr. Rhea writes monthly white papers on various sections of the HIPAA regulations in regard to those most encountered in office practice. The information will be summarized from actual federal law with both references and multiple choice questions for your teaching use.

HIPAA training is required by the regulations must be ongoing and this monthly information can be used as part of efforts to meet those requirements. These HIPAA articles can be used and documented as part of your staff and administrative training program.

While these educational materials will not by any means cover everything you need to do for HIPAA privacy and security compliance they provide more documented evidence of training and intent to comply.

If you have any questions on the information Dr. Rhea can be contacted directly.
krheamd@mdriskconsulting.com

absolute requirement for further investigation. Should the investigation prove the suspicion of willful neglect to be correct the resultant penalties would be in one of the highest categories. In this situation the planned intent to ignore even part of the HIPAA regulations would almost certainly constitute willful neglect.