United Actuarial Services, Inc.
Actuaries and Consultants

2013-31

May 30, 2013

BENEFIT NEWS BRIEFS

Breach of Security Rule Basics Costs Provider $400,000

A recent settlement involving the breach of unsecured electronic protected health information (ePHI) of approximately 17,500 patients serves as a reminder of the importance of observing the *HIPAA Security Rule* basics.

Failure to do so can be co$tly.

Just ask Idaho State University (ISU) which has agreed to pay $400,000 to the U.S. Department of Health and Human Services (HHS) to settle alleged violations of the *Security Rule.*

The HHS Office for Civil Rights (OCR) opened an investigation after ISU notified HHS of the breach in which the ePHI of approximately 17,500 patients was unsecured for at least 10 months, due to the disabling of firewall protections at servers maintained by ISU. OCR's investigation indicated that ISU's *risk analyses* and *assessments* of its clinics were *incomplete* and *inadequately identified potential risks or vulnerabilities*. ISU also failed to assess the likelihood of potential risks occurring.

In particular, HHS' investigation indicated that the following conduct occurred:

- ISU did not *conduct an analysis of the risk* to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012;
- ISU did not *adequately implement security measures* sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and
- ISU did not *adequately implement procedures to regularly review records of information system activity* to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: *mewing@unitedactuarial.com*

http://www.unitedactuarial.com

In addition to the monetary penalty, ISU agreed to a plan of corrective action. The Resolution Agreement can be found on the OCR website at: *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.html*. Some of the items ISU agree to do, usually within 30-60 days of the agreement, include:

Risk Management

> ISU shall provide HHS with its most recent *risk management plan* that includes specific security measures to reduce the risks and vulnerabilities to a reasonable and appropriate level for all of its covered health care components.
>
> Upon receiving notice from HHS either approving or specifying any required changes, ISU shall make the required changes accordingly and promptly implement the *risk management plan*, including any *applicable training*, in accordance with its applicable administrative procedures.

The *Security Rule* addresses risk management plans at Section 164.308 Administrative safeguards, which states a covered entity must implement policies and procedures to prevent, detect, contain, and correct security violations. This Section of the *Security Rule* implementation specifications addresses the following four required areas of compliance:

(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.

(B) ***Risk management*** (**Required**).
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

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

(D) ***Information system activity review*** (**Required**).
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

General *Security Rule* guidance is available from OCR at: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.*

Reference works are available for risk analysis, risk management and information system activity review, as well as on contingency plans. This reference provides more detail on the basics of risk analysis and risk management. In light of OCR increased enforcement activities, covered entities, including multiemployer group health plans would do well to review their risk analysis and risk management activities on an annual basis.

Information System Activity Review

> ISU shall provide HHS with documentation of implementation of its policies and procedures regarding *information system activity review* across all of its covered health care component clinics.
>
> Upon receiving any required changes to such implementation from HHS, ISU shall have 30 days to revise its implementation strategy and provide it to HHS for review and approval.

As noted above, the *Security Rule* addresses ***Information system activity review*** Section 164.308. This implementation specification requires covered entities to "*Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports."*

Compliance Gap Analysis

> ISU shall provide documentation of its updated *compliance gap analysis* activity entitled *Post Incident Risk Assessment,* as specified by HHS, indicating changes in compliance status regarding <u>each</u> Security Rule provision.
>
> Such documentation shall include, but is not limited to, a *copy of the contingency plan* and the *documents implementing the contingency plan* as well as a listing of all technical safeguards implemented and the documents implementing the technical safeguards, across its covered health care clinics.

As part of compliance with the *HIPAA Privacy and Security Rules*, the first step for a covered entity to take is to perform a "*gap analysis*." This analysis measures the *Privacy* or *Security Rul*es requirements against the covered entities current operations and notes the "*gap*" between operations and compliance.

The next step is to systematically fill in the gap with needed policies and procedures. Here, ISU will need to take a look at each aspect of the *Security Rule* and compare that to its operations and close the gap. Numerous *Privacy* and *Security Rule* resources are available from the OCR website located at: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html*.

Annual Reports

As part of the settlement, ISU shall also submit to HHS an Annual Report which shall include, among other things:

- A summary of the *risk management plan* and *security measures* taken during the Reporting Period, including *documentation of training* related to those measures.
- A summary of the *information system activity review measures*, including *documentation of training* related to those measures.
- An update of the *compliance gap analysis* activity conducted.

Since the issuance of the *Final HIPAA Security Breach* rules and other adjustments to the *HIPAA Privacy* and *Security Rules,* most multiemployer group health plans will be reviewing their *Privacy* and *Security Policies* and *Procedures* for needed updates. This would be a good time for such health plans to review their "gap analysis" and other security measures and document any training given to staff.

> "*Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program*," said OCR Director Leon Rodriguez. "*Proper security measures and policies help mitigate potential risk to patient information*."
> Source: HHS News Release
> *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html*

Other information on OCR enforcement activities is available at: *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html*.

*   *   *

LEGAL DISCLAIMER: Information contained in this publication is not legal advice, and should not be construed as legal advice. If you need legal advice upon which you can rely, you should seek a legal opinion from your attorney.