United Actuarial Services, Inc.
Actuaries and Consultants

2012-54

November 2, 2012

CLIENT BULLETIN

Security Rule Enforcement Continues
Provider Tagged in $1.5 Million Settlement with HHS

The Office for Civil Rights (OCR) recently concluded an enforcement action against two Massachusetts medical care providers for $1.5 million dollars for "potential violations" of the *Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule*. The settlement agreement can be accessed at: *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html* or by "*clicking here.*"

This enforcement action should $erve as a reminder to all covered entities to exert continued diligence in their ongoing *Privacy* and *Security Rule* efforts. Business Associates of covered entities should also take note since they are now directly covered by sections of the Security Rule pursuant to the *Health Information Technology for Economic and Clinical Health Act (HITECH) Act*. For additional information on *Privacy* and *Security Rule* compliance see *Benefit News Brief 2012-38* (OCR compliance protocols) and the Research Department's *Topical Index* at *http://www.unitedactuarial.com/research/docs/topical_index/topind_pdflinks.pdf*, pages 11 and 12.

Generally speaking, covered entities are health care plans, health care providers and health care clearinghouses. Business Associates are entities that perform various tasks for covered entities that entail the use of Protected Health Information (PHI).

The OCR investigation was prompted by a "breach" report submitted by the providers pursuant to the *HITECH Breach Notification Rule*. The report noted the theft of an unencrypted personal laptop containing the electronic PHI (ePHI) of the providers' patients and research subjects and included patient prescriptions and clinical information.

OCR's investigation concluded the providers failed to take necessary steps to comply with the *Security Rule* as the providers did not demonstrate that they conducted a thorough analysis of the risk to the confidentiality of ePHI on an *on-going basis* as part of its security management process from the compliance date of the *Security Rule*.

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

In particular, the providers did not:

- fully evaluate the likelihood and impact of potential risks to the confidentiality of ePHI maintained in and transmitted using portable devices,
- implement appropriate security measures to address such potential risks,
- document the chosen security measures and the rationale for adopting those measures, and
- maintain reasonable and appropriate security measures on an on-going basis.

Additionally, the providers:

- security measures were not sufficient to ensure the confidentiality of ePHI that it created, maintained and transmitted using portable devices to a reasonable and appropriate level.

- did not adequately adopt or implement policies and procedures to address security incident identification, reporting and response.

- did not adequately adopt or implement policies and procedures to restrict access to authorized users for portable devices that access ePHI or to provide it with a reasonable means of knowing whether or what type of portable devices were being used to access its network.

- did not adequately adopt or implement policies and procedures governing the receipt and removal of portable devices into, out of, and within the facility. Thus, the providers had no reasonable means of tracking non-provider owned portable media devices containing its ePHI into and out of its facility, or the movement of these devices within the facility.

- did not adequately adopt or implement technical policies and procedures to allow access to ePHI using portable devices only to authorized persons or software programs.

- did not implement an equivalent, reasonable, and appropriate alternative measure to encryption that would have ensured confidentiality of its ePHI or document the rationale supporting the decision not to encrypt.

The investigation indicated that these failures had continued over an extended period of time. OCR stated this demonstrated a long-term, organizational disregard for the requirements of the *Security Rule*. No doubt this continuing violation was a factor in the size of the settlement.

The above bullets detailing the providers' failings can be used as a "check" for covered entities, including multiemployer health plans, to do a self-audit on any similar use of portable electronic devices and ePHI. In addition, PDF pages 10 and

11 of the settlement agreement list what OCR considers to be the minimum policies and procedures concerning such devices. TIP: check your own policies.

The use of such devices and any portable device should be a special concern given the devices ability to hold data on millions of individuals. In the OCR Press Release, OCR Director Leon Rodriguez was quoted as saying:

> "In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices. This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom." (emphasis added)

The settlement agreement also called for the providers to follow a corrective action plan, which includes reviewing, revising, and maintaining policies and procedures to ensure compliance with the Security Rule. An independent monitor will conduct assessments of the providers compliance with the corrective action plan and render semi-annual reports to the government for 3 years.

Additional information about OCR's enforcement activities, including the case examples listed below, can be found on the OCR website at: *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html*

Case Examples Organized by Covered Entity	***Case Examples Organized by Issue***
▪ General Hospitals ▪ Health Care Providers ▪ Health Plans / HMOs ▪ Outpatient Facilities ▪ Pharmacies • Private Practices	▪ Access ▪ Authorizations ▪ Business Associates ▪ Conditioning Compliance with the Privacy Rule ▪ Confidential Communications ▪ Disclosures to Avert a Serious Threat to Health or Safety ▪ Impermissible Uses and Disclosures ▪ Minimum Necessary ▪ Notice • Safeguards

* * *