HHS Doles Out $5.3 Million in Fines for HIPAA Violations in One Week

The US Department of Health and Human Services (HHS) is serious about protecting and enforcing individual rights guaranteed by the HIPAA Privacy Rule. If you had any doubts, simply take a look at the recent fines imposed by the Office of Civil Rights (OCR).

On February 22nd, Cignet Health of Maryland was fined $4.3 million by the OCR – $1.3 million for failure to provide 41 patients with access to their medical records, and another $3 million for not complying with the investigation. This is the first instance of civil monetary penalties being imposed under the Privacy Rule. Cignet was fined for “willful neglect” with the Privacy Rule.

- Cignet refused to respond to federal investigator demands for records, even after a subpoena was issued. It was not until investigators obtained an order from federal court to enforce the subpoena that Cignet complied.
- Cignet turned over 4,500 unrelated patient records in response to the 41 requested. The other records are being held at a federal facility until Cignet takes the proper steps as custodian to ensure their protection.

On February 24th, Mass General agreed to pay HHS a $1 million resolution fine and comply with a corrective action plan for a 2009 incident in which documents containing PHI for 192 infectious disease patients were lost after an employee left them on a subway train. A patient complaint led to an OCR investigation. OCR concluded:

- Mass General “failed to implement reasonable and appropriate safeguards to protect the privacy of PHI when removed from Mass General’s premises, and impermissibly disclosed PHI.”
- The hospital must develop and implement health information protection policies, train its personnel, perform compliance audits, and submit semi-annual reports to the OCR for three years, as part of its corrective action plan.

The OCR, by levying more civil penalties in February than it has in over five years, seeks to make it very clear that Covered Entities must protect their patient’s health information, and that there will be consequences for failure to enact HIPAA’s privacy and data security requirements. “The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules,” warned OCR Director Georgina Verdugo.

Source: HHS Office of Civil Rights
HIPAA Breach Statistics

HHS reported 250 breaches of health data affecting over 6.5 million individuals in just one month. These only include paper and electronic incidents affecting more than 500 individuals, so the true numbers are even greater.

| Health Data Breaches Reported to HHS (affecting > 500 individuals from 1/18/2011 – 2/17/2011) |
|---|---|---|
| # Breaches | Breach Type | # Individuals Affected |
| 135 | Theft | 3,699,822 |
| 54 | Unauthorized Access | 787,398 |
| 42 | Loss | 1,216,468 |
| 21 | Hacking / IT Incident | 903,889 |
| 14 | Improper Disposal | 81,859 |
| 1 | Other | 344,579 |

Editor’s Note: Breaches are attributed to multiple reasons, so the numbers attributed to any one cause will overstate the total in any one category.

Source: HHS, as reproduced by Melamedia

Did you know?
- 10% of all laptops are lost or stolen annually; 98% of those are never recovered
- 66,000 individuals, on average, are affected by a single breach of portable media
- Data breaches cost health care organizations over $8 million annually, on average
- The cost of a breach of one medical record is $214, on average

Sources: HHS, Redspin, Zurich, Ponemon Institute, zTrace Technologies

What Types of Electronic Devices Store ePHI?

The list of electronic devices with the capability to store protected health information is staggering. Here’s just a short list. As you review it, ask yourself the following:

1. How many of these items do I use on a regular basis?
2. What types of ePHI am I placing on the device, and is it only the minimum amount necessary?
3. Do I need to store this ePHI on the device, or can I delete it after some time?
4. Is the device encrypted, password protected, and physically secured?
5. What am I doing operationally and from a privacy and security standpoint to safeguard the PHI on this device?

- Laptop Computers
- Hard Drives
- iPods
- Voice Recorders
- Printers of all kinds
- Desktop Computers
- Flash Drives
- CDs and DVDs
- Dictation Devices
- Answering Machines
- PDAs
- Digital Cameras
- Floppy Discs
- Copy Machines
- X-Ray Machines
- Mobile Phones
- SD Memory Cards
- Magnetic Tapes
- Fax Machines
- MRI Machines
- Pagers
- Video Cameras
- VHS Tapes
- Scanners
- Handheld Pulse Oximeters

For more information go to [http://hipaa.ucsf.edu](http://hipaa.ucsf.edu) or email the Privacy Office at privacy@ucsf.edu
Visitors and Observers

As a world class research, educational, and patient care institution, we often welcome visitors into our space to learn, observe, and otherwise collaborate. However, we must also take the right precautions to protect our patients’ privacy, confidentiality, safety, and standard of care. Guidelines have been developed by Human Resources, Risk Management, Legal Affairs, and Privacy to ensure the consistent and appropriate handling of visitors. Find the checklist at http://hr/departments/employment/compliance.aspx. Links to additional forms and information can be found at http://hipaa.ucsf.edu/education/visitors. For questions or guidance, please contact Human Resources, Risk Management, Occupational Health, and/or Privacy Office.

Delayed Launch of HITECH Final Rules

Late last year, HHS indicated that it planned to issue the final HIPAA modifications in March of 2011. It now appears the release will be delayed until Q3 or Q4 of 2011, as OCR intends to release all modifications at the same time, including those for HIPAA privacy and security, enforcement (the HIPAA compliance audit program), and breach notification.

However, on February 9th, HHS forwarded the proposed rule on Accounting of Disclosures in Electronic Health Records to the Office of Management and Budget (OMB). The OMB review may take up to 90 days, after which the rule will be finalized and published. The rule will lay out what healthcare providers will be held accountable for when patients request an accounting of disclosures of their electronic health record, which HITECH expanded to include disclosures made for purposes of treatment, payment, and operations.

Source: HHS Office of Civil Rights, Health Leaders Media, HIPAA Weekly Advisor

The Privacy Office Website

You have privacy questions and concerns. We have answers! Call us anytime at (415) 353-2750, or visit our website at http://hipaa.ucsf.edu for a host of resources and information. Find training guides, policies and procedures, forms, research and IT Security guidance, HIPAA FAQs, the Privacy Handbook, the Notice of Privacy Practices, UCSF privacy news and newsletters, resources and links, and contact information, all designed to help you protect our patients’ medical, personal, and sensitive information.

For more information go to http://hipaa.ucsf.edu or email the Privacy Office at privacy@ucsf.edu