Healthcare needs responsible ITAD

Where do your computers go when they are disposed? How about the data?

Did you know that HIPAA requires Covered Entities to have policies and procedures in place to govern the disposal of IT Assets and the Personal Health Information on these devices? How well do you comply?

The Office for Civil Rights (OCR) is in the midst of conducting its Phase 2 desk and on-site audits of approximately 350 Covered Entities (including health care providers, health plans, and health care clearinghouses). OCR is a part of the US Department of Health and Human Services (HHS) and it investigates and enforces compliance with HIPAA/HITECH (among other things).

The scope of the audits is published on the HHS web site *(http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html)* and provides a glimpse into what organizations must do to prepare themselves for the audits and to be in compliance with the law.

Breaches are costly

Since 2011, 1,672 breaches impacting ≥500 people reported to OCR:

- ~45% involved theft and/or loss
- ~29% involved unauthorized access/disclosure
- ~17% involved hacking/IT incident
- Estimated cost to the health care industry in 2012: $7 billion

10/7/16, Third Annual Benchmark Study on Patient Privacy & Data Security study by The Ponemon Institute

IT Asset Disposition ("ITAD") aspects of the organization (Section 164.310(d)(1) of HIPAA) are a required element of the regulation that is likely to be included in any audit.

OCR's audit protocol states it will: *"Inquire of management as to how the disposal of hardware, software, and ePHI data is managed. Obtain and review formal policies and procedures and evaluate the content relative to the specified criteria regarding the disposal of hardware, software, and ePHI data. Obtain evidence, on a sample basis, to determine whether the entity had oversight policies and procedures that address how management verifies that disposal policies are being carried out."*

According to *Government Health IT,* the first round of OCR audits in 2013 found that **89% of audited organization had identified failures or weaknesses under the requirements.** *(http://www.healthcareitnews.com/news/steps-prep-phase-2-ocr-audits)*. This publication goes on to recommend Covered Entities get their houses in order for Phase 2 audits by working with Business Associates to develop and maintain a culture of compliance with HITECH throughout the "business ecosystem."

How will you protect your institution and your patients?

See other side for details

Madison, WI * Indianapolis, IN
608-222-4800 * 888-222-8399
info@cascade-assets.com * www.cascade-assets.com

To be prepared, Covered Entities should partner with their ITAD vendors on the following items:

- Review and execute an up-to-date **Business Associate Agreement** - if a vendor collects any computer or equipment that may have PHI, you MUST have a BAA in place with that vendor. Note, even if it's your policy to destroy PHI data in-house before it leaves your control, a BAA should still be put into place in case any unwiped media slips through.
- Review and update your **Security Policy** - this policy should be reviewed every year and should cover the ever-increasing array of data storage devices likely to contain PHI and current media sanitization standards. If your policy only covers computer hard drives or references the legacy Department of Defense 5220.22-M standard, then your policy is out of date! Review your policy to ensure it incorporates current NIST 800-88 Guidelines and covers all affected media.
- Have access to **disposition records or Certificates of Destruction** - if you are audited, you may need to provide evidence that any data storage devices sent to your Business Associate were properly destroyed. Many firms provide destruction records via on-line tools or through electronic or paper reports.
- Ensure proper **destruction of electronic medical records** - the life cycle of electronic medical records is now considered more explicitly. Thus, data "In Disposal" is regulated, requiring methods of destruction that render data "unrecoverable" and "indecipherable". Although the HIPAA standards are technology neutral, the guidance offered is to follow the destruction standards recommended in the NIST 800-88 Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
- Conduct proper **due diligence** on your Business Associate - Covered Entities need to demonstrate they are contracting with firms that have reasonable controls in place to prevent the loss of PHI and to properly respond in the event of a suspected data breach. Either perform the due diligence yourself with an on-site audit and/or find a provider with the appropriate **NAID Certification**, which requires annual and unannounced on-site audits of firms to verify their qualifications in data destruction.

Non-compliance is also costly

You don't have to have a breach to be fined by OCR for non-compliance

- $1.55m fine to North Memorial Health Care of MN for not having a BAA with contractor and not performing a risk analysis (March '16)
- $5.55m settlement and corrective action plan with Advocate Health Care due to absense of risk analysis, no P&Ps to limit access to info systems, and no BAA in place with billing vendor (September '16)

Additional References:

- The Department of Health and Human Services put together a list of disposal FAQ's: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf
- Free BAA Templates and Data Security Policies are available for download at: http://cascade-assets.com/healthcare/

Madison, WI * Indianapolis, IN
608-222-4800 * 888-222-8399
info@cascade-assets.com * www.cascade-assets.com