ISSUE BRIEF

OCR Audit Documentation Requests – What We Know Now

It is now the end of April 2012, and the first 20 OCR audits that were completed at the end of January are under review. As you remember the audits cover HIPAA security, breach, and privacy only! Everyone is an audit target, all covered entities, and all business associates. The first round did not include business associates.

The information that OCR has released can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. It includes nothing more than an initial sample letter at, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/sample-ocr_notification_ltr.pdf.

There is nothing new on these websites since our first issue brief on this topic. OCR did say at several conferences that they would be reviewing the first 20 audits and updating the protocols and documentation for use in the next series of audits, perhaps as many as 130 more by the end of 2012.

One of the items included in the OCR and KPMG letter that went to all of the first 20 audited was a several-page document request. It outlines the scope to a finer granularity (but remember this was the first step.) There was also an on-site visit or series of visits, where more documentation could be requested.

The document list below is what was sent to one of the first 20 entities audited. You will see that it begins with some basic business information, then HIPAA Security, next HIPAA Privacy, and something called **HITECH** Organizational Process-Based Capabilities, which refers to breach notification.

Please note that the document request included the policies, procedures, plans and other items required by the regulations, **and** evidence that the policies and operational procedures have been implemented.

We cannot corroborate that the document requests was the same for all 20 entities audited, nor if it was the same for the same type of covered entity, nor if it will be the same for a business associate that are audited in the future.

We suggest you begin active preparation for potential audit by reviewing your ability to produce the documentation on the list and next review all your organization's policies, procedures and documentation that might reasonably be produced to enable auditing that verifies implementation of all required policies.

It appears that OCR is going to be knocking on everyone's digital door in the near future. It appears that OCR will audit all covered entities and business associates periodically.

You will need to stay tuned to the OCR websites outlined above, the MalvernGroup Alerts, and consider a one-month-free subscription to Sue Miller's weekly Healthcare Information Report to find out if and how the document request has changed.

Checklist Category	Document Name/Description
General Information	
General Information	Size of Covered Entity: # of employees, members or patients, facilities, EMR facility (Y/N)
HIPAA Security	
General Governance – HIPAA Security	Identify any applicable industry guidance (e.g., studies, practices, regulations, etc…)or other reference material used to develop any of the policies and procedures requested below (NO NEED TO PROVIDE THIS DOCUMENTATION – SIMPLY IDENTIFY)
General Information – HIPAA Security	Security Officer Contact Information (name, email, phone, address and admin contact info)
Administrative Safeguards	Entity-Level Risk Assessment
Administrative Safeguards	Organization Chart
Administrative Safeguards	Information Security Policies, specifically those documenting security management practices and processes such as: - Access Control - Data Protection - Acceptable Use - Workstation Security - Workforce/HR Security - Sanction Procedures
Administrative Safeguards	Security Incident Management Plan
Administrative Safeguards	Business Continuity/Disaster Recovery Plan
Administrative Safeguards	Data backup and recovery procedures
Physical Safeguards	Physical Security Policies and Procedures
Physical Safeguards	Data destruction and media reuse procedures
Technical Safeguards	Encryption policies and procedures
Technical Safeguards	Management's internal control/internal audit policies and procedures relative to monitoring IT safeguards
Technical Safeguards	System-generated user access listing of all individuals with access to systems housing EPHI
Technical Safeguards	System-generated listing of all New Hires within the past year
Technical Safeguards	User authentication policies and procedures
HIPAA Privacy	
General Governance – HIPAA Privacy	Identify any applicable industry guidance (e.g., studies, practices, regulations, etc….) or other reference material used to develop any of the policies and procedures requested below (NO NEED TO PROVIDE THIS DOCUMENTATION – SIMPLY IDENTIFY)
General Information – HIPAA Privacy	Privacy Officer Contact Information (name, email, phone, address and admin contact info)
HIPAA Privacy	Privacy Policy (s) and Notice of Privacy Practices
HIPAA Privacy	Privacy Practices Documentation including: - Use and Disclosure - Rights to Request Privacy Information - Right to Request Privacy Protection of

	PHI - Access of Individuals to PHI - Denial of Access to PHI Procedures - Amendment of PHI - Accounting of Disclosures of PHI - Administrative Requirements - Transition Provisions
HIPAA Privacy	Training documentation for employees over Privacy Practices and organization training policy(s)
HIPAA Privacy	Policies and procedures in place over administrative, technical and physical safeguards over all forms of PHI
HIPAA Privacy	Complaint handling policies and procedures
HIPAA Privacy	Population of complaints over Privacy practices made within the past year (complaint log)
HIPAA Privacy	Sanction and disciplinary policies and procedures over Privacy violations
HIPAA Privacy	Mitigation and disciplinary policies and procedure for when a breach occurs
HIPAA Privacy	Anti-intimidation/anti-retaliation policies and procedures
HIPAA Privacy	Policies and procedures over Uses and Disclosures of PHI, including: - Deceased individuals - Personal representatives - Confidential communication - Business associate contract requirements - Health Plan documentation requirements - Treatment, payment, and/or operation - Consent and authorization requirements - Judicial or administrative proceeding requirements - Research requirements - Approval or waiver requirements - De-identification/Re-identification of PHI procedures - Restriction of PHI - Minimum necessary requirements - Limited information provided for fundraising purposes - Health care underwriting requirements - Identity verification procedures of individuals requesting PHI
HITECH Organizational Process-Based Capabilities	
HITECH	Breach notification processes, entity-level risk assessment documentation and capabilities