

Indiana Security and Privacy Network (InSPN)

Legal Update – November 17, 2011

*Mark J. Swearingen, Hall Render**

- HIPAA Enforcement Statistics:
 - **Privacy Rule** (through July 31, 2011)
 - 62,708 total complaints
 - 783 in May, 706 in June, and 669 in July
 - 91% resolved
 - 9% remain open
 - 21,430 complaints investigated
 - 14,105 cases of corrective action (66%)
 - 7,325 cases where no violation (34%)
 - Most investigated areas:
 - Impermissible use/disclosure
 - Lack of safeguards
 - Lack of patient access
 - Minimum necessary
 - **Security Rule** (through July 31, 2011)
 - 938 total complaints/reviews
 - 303 open complaints/reviews
 - Most frequent standards at issue:
 - Response and reporting (administrative)
 - Awareness and training (administrative)
 - Access Control (technical)
 - Information Access Management (administrative)
 - Workstation security (physical)
 - **Breach Notification Rule** (through November 17, 2011)
 - 364 breaches of >500 reported to HHS
 - Over half are due to theft
 - Nearly half involve laptops/portable devices
 - About 1/4 involve paper records only
 - 17,965,109 people affected
 - 34,000+ reports of breaches <500
- In the Media:
 - Just last evening and this morning, it is being reported that Sutter Health in California had a desktop computer stolen that contained PHI regarding 4,000,000 individuals. No financial information or social security numbers were included.
 - There's only one P in Peyton!
 - Wendy Mangin's Privacy Report for today discusses several other recent privacy-related items in the media.

- Regulatory Developments/Updates:
 - **HITECH Regulations**
 - We are still awaiting the final regulations dealing with healthcare privacy and security issues, which will be issued in one "omnibus" rulemaking yet this year.
 - **Proposed Rule – CLIA Program and HIPAA Privacy Rule** (September 14)
 - Proposes to amend HIPAA to provide individuals the right to receive their test reports directly from laboratories by removing the exceptions for CLIA-certified laboratories and CLIA-exempt laboratories from the provision that provides individuals with the right of access to their protected health information.
 - **HIPAA Audits**
 - Section 13411 of HITECH requires HHS to periodically audit covered entities and business associates for compliance with the HIPAA Privacy and Security rules.
 - OCR announced a pilot program to audit 150 covered entities, from November 2011 to December 2012.
 - Stated purposes:
 - Assess HIPAA compliance efforts by a range of covered entities
 - Examine mechanisms for compliance
 - Identify best practices
 - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
 - OCR will select a wide range of types and sizes of CEs. Not expected to include Business Associates initially, although they are eligible.
 - CE will receive notice of selection and a request to provide documentation of privacy and security compliance efforts within 10 business days.
 - CE will receive 30-90 days' notice of the onsite visit, which will take from 3-10 business days.
 - CE will have an opportunity to review and comment back to auditor prior to submission of final audit report to OCR.
 - OCR states that main use of the audits will be to better understand compliance efforts with particular HIPAA rules, to determine what types of technical assistance should be developed, and what types of corrective action are most effective.
 - If an audit indicates serious compliance issues, OCR may initiate a compliance review to address the problem.
 - OCR will not publish a list of selected entities or audit findings.

*Contact Mark at mwearingen@hallrender.com or (317) 977-1458.