WINSTON & STRAWN LLP

BLOG

HHS Prepares for HIPAA Audits

MARCH 19, 2014

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) recently announced that it plans to survey up to 1200 HIPAA "covered entities" (e.g., health plans, health care clearinghouses, and certain health care providers) ***and*** "business associates" (i.e., the entities that provide services to covered entities) for the purpose of identifying candidates for audit under the OCR HIPAA Audit Program.

In connection with the pre-audit survey, OCR will request information to assess the size, complexity, and fitness of a given covered entity or business associate for audit, such as data regarding the number of patient visits or insured lives, use of electronic information, revenue, and business locations. OCR is required to conduct such audits on a periodic basis to confirm compliance with the HIPAA privacy, security, and breach notification rules. HHS is accepting comments regarding the pre-audit survey until April 25, 2014. It is unclear when in 2014 the audits will begin.

Here are some examples of what we expect OCR will be looking for in a HIPAA audit:

- Whether formal or informal policies or practices have been adopted to conduct a risk assessment regarding the confidentiality, integrity, and availability of electronic protected health information (PHI);
- Whether an encryption mechanism is in place to protect electronic PHI; if an encryption mechanism is not fully implemented, whether the rationale for taking such approach has been documented, and whether a reasonable alternative has been implemented;
- Whether audit controls have been implemented over information systems that contain or use electronic PHI, and whether documentation exists demonstrating such implementation;
- Whether requirements with respect to personal representatives' access to PHI have been met;
- Whether individuals have been notified of the potential uses and disclosures of PHI;
- Whether a process exists to permit disclosures of PHI by whistleblowers and what the conditions are for such disclosure; and
- Whether a standard template or form letter exists for notifying individuals of breaches of unsecured PHI; and, if breaches have occurred, whether the notices used contain the required elements.

For additional examples, refer to the OCR HIPAA Audit Program Protocol here; however, note that the Protocol has not yet been updated to reflect the Omnibus Final Rule.

1 Min Read

Related Locations

Chicago

Related Topics

Health and Welfare Benefits

Health and Human Services

HIPAA

Related Capabilities

Employee Benefits & Executive Compensation

Health Care

Related Regions

North America

Related Professionals

Erin Haldorson Weber

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.