

Health Information Compliance Alert

HIPAA Breaches: Guard Against IT-Sparked HIPAA Breaches

HHS OCR puts teeth in its fines for HIPAA violations.

Don't let a computer conversion lead to major fines for violating patient privacy. That's what Indianapolis-based managed care company **WellPoint Inc.** has learned the hard way. Wellpoint has agreed to pay \$1.7 million to settle HIPAA charges, the **Department of Health and Human Services** says in a release.

The **HHS Office for Civil Rights** (OCR) started an investigation after WellPoint self-reported that "security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet," HHS says in the release. That data, which was accessible for more than four months, included names, dates of birth, addresses, Social Security numbers, telephone numbers, and health information.

Mind Your Technical Safeguards

The managed care company "did not implement appropriate administrative and technical safeguards" when it made a systems upgrade to an online application database. Namely, it didn't "adequately implement policies and procedures for authorizing access to the on-line application database; perform an appropriate technical evaluation in response to a software upgrade to its information systems; [or] have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database," HHS says.

Warning: "This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet," HHS stresses.

Don't think you can get off the hook for a similar breach by pointing the finger at your software vendor. "Whether systems upgrades are conducted by covered entities or their business associates, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information □ especially information that is accessible over the Internet," the agency says.

However, vendors will have to shoulder more blame for HIPAA breaches when the rules change this fall. "Beginning Sept. 23, 2013, liability for many of HIPAA's requirements will extend directly to business associates that receive or store protected health information, such as contractors and subcontractors," HHS notes.