fyi®

For your information

Volume 35 | Issue 42 | July 2, 2012

HIPAA Privacy and Security Update

Recent enforcement and regulatory activity signals that entities subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules should confirm their compliance with the law. First, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) – the government agency responsible for enforcing the HIPAA privacy and security rules – recently fined the Alaska state Medicaid agency $1.7 million for alleged security violations. Similarly, OCR recently finalized the HIPAA audit protocol used to conduct audits of approximately 115 HIPAA-covered entities. This enforcement activity precedes soon-to-be-released final regulations containing a broad range of HIPAA privacy, security, and enforcement rules. These events underscore the need for HIPAA-covered entities – including group health plans and health care providers – to revisit HIPAA compliance and be aware that updates to HIPAA documents and procedures may be necessary in the near future.

First HIPAA-related enforcement action against a state agency

The Alaska Department of Health and Social Services – the State's Medicaid agency – agreed to pay HHS $1.7 million to settle alleged violations of the HIPAA security rules. The agency will also take corrective action to safeguard the electronic protected health information (ePHI) of its Medicaid beneficiaries. It also must report to the federal government its progress implementing the corrections. The enforcement action follows a breach report provided by the agency to OCR, which describes a possible HIPAA breach resulting from a stolen portable electronic storage device (USB hard drive) containing ePHI. During its investigation, OCR determined that the agency had not complied with several other security requirements, including adequate policies and procedures, risk analysis, device and media controls, and workforce security training. This enforcement action is a reminder to all HIPAA-covered entities that the government is actively pursuing possible HIPAA breaches and that noncompliance could result in significant penalties.

Audit program

OCR implemented a pilot audit program in late 2011 to review compliance with HIPAA's privacy and security rules and the breach notification standards. This program was required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The accounting firm KPMG

was awarded the contract to develop the program and conduct approximately 115 audits of HIPAA-covered entities from late 2011 through 2012.

INSIGHT

OCR's audit program does not affect a person's right to file a complaint directly with OCR, which may spark a separate investigation.

Audit protocol finalized. OCR published a comprehensive audit protocol that contains the procedures that were followed during the audits. The protocol is organized around modules, representing separate elements of the privacy, security, and breach notification requirements. The choice of module used during an audit depends on the covered entity selected for review.

INSIGHT

This completed protocol may signal longer-term audit activity after the pilot program ends, and covered entities should confirm their compliance with the law.

Additional HIPAA guidance coming soon…

While enforcement activity heats up, HHS is in the last stages of publishing final omnibus regulations. Regulators have said that these regulations will include:

- Enforcement and penalty rules
- Updated privacy and security rules required by the HITECH Act
- Final rules on breach notification
- Changes to HIPAA stemming from the Genetic Information Nondiscrimination Act.

Regulators also said that these regulations may include further guidance on the use of protected health information (PHI) in marketing, prohibitions related to the sale of PHI, data-breach harm threshold, and encryption. As a result of these final regulations, covered entities may need to update required HIPAA documents and administrative procedures, including HIPAA policies and procedures, privacy notices, and business associate agreements.

Conclusion

This recent HIPAA enforcement and regulatory activity provides a stern reminder to HIPAA-covered entities that noncompliance can have significant consequences. It also underscores the need for covered entities to revisit their HIPAA compliance and be ready for the updates that may be necessary in the near future.

Buck Can Help

- Assist employers determine if they are HIPAA compliant
- Review HIPAA documents to determine if they include required content
- Train workforce employees