HHS ANNOUNCES $1.5 MILLION HIPAA ENFORCEMENT ACTION

On March 13, 2012, the Department of Health and Human Services ("HHS") announced that it had reached a settlement with Blue Cross Blue Shield of Tennessee ("Blue Cross") arising from potential violations of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Notably, HHS learned of the circumstances giving rise to the enforcement action through the notification provided by Blue Cross to HHS under the HITECH Breach Notification Rule. This marks the first enforcement action arising from information divulged to HHS under the Breach Notification Rule, which was required by the Health Information Technology for Economic and Clinical Health Act ("HITECH").

The underlying facts involved the theft of 57 unencrypted computer hard drives from a data closet at a former Blue Cross call center in October 2009. The hard drives contained both audio and video files of customer service calls received by Blue Cross. The information in those files included the names, dates of birth, social security numbers, diagnosis codes and health plan identification numbers for 1,023,209 Blue Cross members. Blue Cross notified the affected individuals and HHS as required by the HITECH Breach Notification Rule.

The HHS Office for Civil Rights ("OCR") investigated the reported breach and found that Blue Cross had failed to implement appropriate administrative safeguards to adequately protect information in the data closet by not performing the required security evaluation in response to operational changes. OCR also found that Blue Cross had failed to implement appropriate physical safeguards by not having adequate facility access controls in place. As a result, OCR and Blue Cross entered into a Resolution Agreement whereby Blue Cross agreed to pay HHS a $1,500,000 settlement payment and to perform the following additional obligations:

- Review and revise its privacy and security policies and obtain HHS approval of the same, which policies and procedures must cover: the conduct of a risk assessment and a risk management plan; physical access controls; and physical safeguards governing the storage of electronic storage media containing electronic protected health information;
- Conduct regular and robust workforce training, and not permit any member of the Blue Cross workforce to work in areas involving the storage or transport of media and devices containing electronic protected health information until the workforce member executes a specified training certification;
- Perform internal monitor reviews under the direction of the Blue Cross Chief Privacy Officer; and
- Submit biannual reports indicating compliance with the terms of the Resolution Agreement.

In the press release announcing this enforcement action, OCR Director Leon Rodriguez was quoted as saying that "OCR expects health plans and health care providers to have in place a carefully designed, delivered and monitored HIPAA compliance program." He also indicated that OCR would continue to use the HITECH Breach Notification Rule as an enforcement tool to vigorously protect patient privacy. In light of this development, covered entities should take the necessary steps to ensure that their HIPAA compliance programs are in good shape, including:

- Conducting a risk assessment to determine where vulnerabilities exist in current practices, systems and structures;
- Reviewing policies and procedures affecting privacy and security to ensure that they are thorough, complete and communicated to workforce members;
- Actively monitoring compliance, particularly when there is a material change in processes, personnel or functions;
- Consistently enforcing policies and procedures when conduct occurs that violates them; and
- Considering the use of encryption for all media and devices that store, transmit or maintain protected health information.

More information on this enforcement action, including the Resolution Agreement and the HHS press release, is available here.

Hall Render's HIPAA Impact Series has provided in-depth analysis of HIPAA issues and developments since the passage of HITECH. Our HIPAA Impact Series may be accessed at: www.hallrender.com/impact.

If you need additional information about HIPAA/HITECH, please contact Mark J. Swearingen at 317.977.1458 or mswearingen@hallrender.com or your regular Hall Render attorney.