March 22, 2012

$1.5 Million Settlement with U.S. Department of Health and Human Services for Alleged Privacy and Security Rule Violations is Yet Another Reminder to Develop HIPAA Compliance Procedures

In the first of its kind, on March 13, 2012, the Department of Health & Human Service ("HHS") announced the settlement of a HIPAA large breach case (affecting over 500 individuals) with Blue Cross Blue Shield of Tennessee ("BCBST") for a record $1.5 Million. The settlement was the result of BCBST's self-disclosure of a potential HIPAA violation under the newly promulgated Health Information Technology for Economic and Clinical Health ("HITECH") Act Breach Notification Rules, and represents the maximum civil monetary penalty ("CMP") that may be imposed in a single calendar year for all identical violations of the HIPAA rules.

Following BCBST's self-disclosure of the theft of 57 unencrypted hard-drives containing electronic protected health information ("e-PHI" or "PHI") of more than one-million BCBST subscribers, including names, social security numbers, diagnoses, birth dates and health plan identification numbers, HHS's Office of Civil Rights ("OCR") conducted an investigation, which ultimately revealed that BCBST failed to have adequate administrative and physical controls over its members' e-PHI. Among the failures identified in OCR's investigation were: (1) BCBST's failure to perform the requisite security evaluation of the leased facility in response to operational changes to ensure adequate protection was in place for e-PHI housed there; and (2) failure to maintain adequate facility access controls over the e-PHI. In addition to a $1.5 Million settlement, BCBST has entered into a rigorous Corrective Action Plan ("CAP") with HHS to address delinquencies in its HIPAA Compliance program.

Among the compliance measures imposed under the CAP are the following actions:

- BCBST must revamp its HIPAA Privacy and Security policies and programs to meet federal mandates and obtain approval of the same from HHS prior to implementation.
- Within 40 days of HHS's approval of the policies, BCBST must provide the policies to all members of its workforce that have access to PHI and obtain written certification of receipt from each individual.
- BCBST must provide training to its workforce on its HIPAA policies and obtain written certification by each individual that such training was completed.
- Employees are precluded from accessing or possessing PHI until they receive the policies and requisite training and execute the mandatory certifications.
- BCBST is required to undergo two random (unannounced) Monitor Reviews to ensure that it is adhering to its HIPAA policies and the CAP. These Monitor Reviews will include, among other things:
    - Audits of portable devices and storage media

- Site visits at BCBST facilities that house portable devices;
- Interviews of employees who use portable devices;
- Two bi-annual reports to HHS on BCBST Compliance efforts; and
- A three-year document retention.

The Agreement also includes a tolling of the six-year Statute of Limitations to enable HHS to pursue the full range of penalties available for HIPAA violations in the event BCBST breaches the CAP.

Given the extensive penalties and administrative burdens that the BCBST settlement establishes, coupled with the ensuing HIPAA audits that will be conducted by an accounting firm, now is the time for HIPAA covered entities to take the time and review their HIPAA policies and the manner in which they are being carried out. According to HHS OCR Director Leon Rodriguez, the BCBST Settlement "sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program."

HIPAA Enforcement Activity.

The HITECH Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information (a "breach") of 500 individuals or more to HHS and the media no later than 60 days following the breach. Smaller breaches affecting less than 500 individuals must be reported to HHS on an annual basis.

While the BCBST settlement was the first of its kind under the HITECH notification rules, it is by no means a novel concept that will pass any time soon. The following is just a small sampling of the HIPAA enforcement actions that have transpired in recent years:

- **Minnesota Attorney General Lawsuit**—In January 2012, the Minnesota Attorney General filed suit against Accretive Health, Inc., a business associate performing revenue cycle activities for two hospital systems, for, among other things, failing to protect the confidentiality of patient health care records. The case arose after an Accretive employee left an unencrypted laptop containing sensitive information on 23,500 patients of the two hospital systems in a rental car, which laptop was later stolen.

- **$4.35M Civil Money Penalty for Failure to Provide Access and Failure to Cooperate in Investigation.**—In February 2011, HHS-OCR imposed a civil money penalty ("CMP") of $4.3 million on Maryland-based Cignet Health for violations of the HIPAA Privacy rule and failure to cooperate with OCR's investigation. The OCR began its investigation of the health center after multiple individuals complained to OCR that the health center refused to grant their requests for copies of their medical records. Ultimately, OCR determined that the covered entity had failed to provide 41 individuals with access to copies of their PHI, in violation of the HIPAA Privacy rule. Under the rule, each day that a violation continues (i.e., each day that access was not provided) for each individual is treated as a separate violation. OCR detailed the health centers complete failure to cooperate with, or even respond to, any aspect of OCR's investigation. OCR found that the failure to cooperate resulted from "willful neglect" of obligations under HIPAA. In determining the penalty, OCR noted two significant factors: First, the violations hindered the ability of individuals to obtain continuing health care (because they sought copies of their PHI in order to share with new providers), and second, the failure to cooperate with the investigation forced OCR to issue a subpoena and file a petition with the court.

- **$1M Settlement with Massachusetts's Hospital for Employee's Loss of Patient Records**—In February 2011 (only 2 days after the announcement of the Cignet CMP), HHS announced another settlement with a Massachusetts hospital, whereby the hospital agreed to pay $1 million to settle potential violations of the HIPAA

Privacy and Security rules. The basis for the action was the hospital's loss of PHI involving 192 patients. In order to work on cases from home, a hospital employee removed from hospital premises patient encounter forms that included 66 patients' names, dates of birth, medical record numbers, health insurers and policy numbers, diagnoses, and the names of the providers. In addition, the employee took home the practice's daily office schedules for three days containing the names and medical record numbers of additional patients. While commuting to work on the subway, the employee placed the 192 files on the seat next to her and subsequently exited the subway and left the files on the seat in the subway. The files were never recovered.

- **Hospital Fined $865,500 for Employees' Curiosity**—In July 2011, HHS announced a settlement of $865,500 with University of California at Los Angeles Health System ("UCLAHS") for potential violations of the HIPAA Privacy and Security Rules, together with a corrective action plan aimed at remedying gaps in UCLAHS's compliance program. The settlement resolved two complaints filed with OCR on behalf of two celebrity patients who received care at UCLAHS. The complaints alleged that UCLAHS employees repeatedly and without permissible reason looked at the electronic protected health information of these patients. OCR's investigation revealed that from 2005-2008, unauthorized employees repeatedly looked at the e-PHI of numerous other UCLAHS patients.

While the HIPAA Privacy and Security rules are not new, the increased enforcement action is new and should re-awaken one's attention to the rules.

Perhaps even more significantly, it is anticipated that in the very near future, HHS will issue guidance allowing the sharing of penalties with complainants (i.e., those harmed by the Privacy or Security rule violations). This sharing will provide an incentive to individuals to report to HHS what they perceive as violations of the Privacy (or Security) rules.

Currently, the HIPAA Privacy rule applies to "covered entities" which are generally defined as follows:

- **Health Plans**, including employer-sponsored group health plans, government and church-sponsored health plans, and multiemployer health plans.

- **Health Care Providers (institutional and non-institutional providers)** that electronically transmits health information in connection with a "standard transactions" either directly or through a third-party billing service.

- **Health Care Clearinghouses** that process nonstandard information received from another entity into a standard (i.e., standard format or data content), or vice versa and include billing services, repricing companies, community health management information systems, and value-added networks.

- **Business Associates.** Effective February 17, 2010, pursuant to HITECH amendments, Business Associates are required to comply with the HIPAA Privacy and Security Rules. It is anticipated that HHS will issue in the near future new regulations establishing Business Associates' compliance mandates that will, in turn, allow HHS-OCR to commence enforcement actions direct against Business Associates for breaches of the HIPAA rules.

What Information is Protected?

Under HIPPA's Privacy rule, all "individually identifiable health information," or "PHI," held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral is protected from unauthorized use or disclosure. PHI includes demographic data that relates to:

- the individual's past, present or future physical or mental health or condition,

- the provision of health care to the individual, or

- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

HIPAA's Security rule protects a subset of information covered by the Privacy rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form or "e-PHI." The Security rule does not apply to PHI transmitted orally or in writing.

In sum, the tougher enforcement status of governmental regulators sends a clear message to applicable parties that it is time to ensure they have developed and implemented policies compliant with the HIPAA Privacy and Security rules.

Additional information, including publications and alerts about HIPAA, HITECH and the administrative requirements of the Privacy and Security Rules is available on Butzel Long's website at www.butzel.com under the Health Care Practice Group.

If you have questions regarding the HIPAA Privacy or Security rules, please contact the authors of this Client Alert, a member of the Butzel Long Health Care Practice Group, a member of the Butzel Long Employee Benefits Practice Group, or your regular Butzel Long attorney.

Debra A. Geroux
248 258 2603
geroux@butzel.com

Thomas L. Shaevsky
248 258 7858
shaevsky@butzel.com

Health Care Industry Group

Robert H. Schwartz
248 258 2611
schwartzrh@butzel.com

Thomas R. McAskin
248 258 2511
mcaskin@butzel.com

Susan H. Patton
734 213 3432
patton@butzel.com

Adele P. Jorissen
248 258 7864
jorissena@butzel.com

Rebecca S. Davies
313 225 7028
davies@butzel.com

The above news is only intended to highlight some of the important issues. This e-mail has been prepared by Butzel Long for information only and is not legal advice. This information is not intended to create, and receipt of it does not constitute, a client-lawyer relationship. Readers should not act upon this information without seeking professional counsel. This electronic newsletter and the information it contains may be considered attorney advertising in some states. If you feel you have received this information in error, or no longer wish to receive this service, please follow the instructions at the bottom of this message.

Attorney Advertising Notice - The contents of this e-mail may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.

For previous e-news or to learn more about our law firm and its services, please visit our website at: www.butzel.com

Butzel Long Offices:
Ann Arbor
Bloomfield Hills
Detroit
Lansing
New York
Washington D.C.

Alliance Offices:
Beijing
Shanghai
Mexico City
Monterrey

Member:
Lex Mundi