EPSTEIN BECKER GREEN | HEALTH CARE & LIFE SCIENCES CLIENT ALERT

Thought Leaders in Health Law®

2012 Privacy and Security Year in Review

by Ross K. Friedberg and Ophir Stemmer

October 2012

In 2012, there has been a continuation of the trend toward heightened regulation and enforcement of the privacy and security requirements under the Health Information Portability and Accountability Act ("HIPAA") and under other state and federal health privacy laws. Although there have not been any significant changes to federal health privacy laws this year, federal enforcement activity continues to be strong.

Recent actions taken by the Department of Health and Human Services ("HHS") suggest that HHS's approach to regulating health information privacy and security is continuing to shift in the direction of enforcement as another way to send a message about the importance of voluntary compliance. In 2012, HHS's Office of Civil Rights ("OCR") entered into a number of highly publicized settlements with HIPAA covered entities ("Covered Entities") stemming from alleged violations of HIPAA. Also this past year, OCR launched a new HIPAA audit and compliance program ("Audit Program"), which it initially intends to use for information-gathering and compliance improvement purposes. In addition, HHS continues to promote better privacy and security practices, most recently by incorporating certain privacy standards relating to medical records access into its electronic health records ("EHRs") incentive program's eligibility requirements.

There also was some notable state activity in 2012, including a new health information privacy law in Texas that, in many respects, is more stringent than HIPAA, and new privacy legislation regarding social media in New Jersey and California that affects employers, including health care employers. Furthermore, there have been additional cases where state attorneys general have brought actions against Covered Entities for alleged HIPAA violations.

Provided below is a summary of these and other related developments over the last year.

A. No Omnibus Rule

Perhaps the greatest news of 2012 in the world of health information privacy and security is what *didn't* happen. The regulations proposed by HHS interpreting crucial portions of HIPAA and the Health Information Technology for Economic and Clinical Health (or "HITECH") Act (popularly referred to as the "Omnibus Rule") remain at the Office of Management and Budget ("OMB") awaiting clearance. Although OMB initially stated that its review would be concluded by late July, OMB extended its review period indefinitely several weeks before the deadline. Among the many important provisions in the proposed final rule is the interpretation of the term "minimum necessary" in the context of the use or disclosure of protected health information ("PHI"). This will have a far-reaching impact on practice and record-keeping for HIPAA-regulated entities. The proposed regulations also will include provisions governing the use of PHI in marketing and the level of data encryption required for electronic systems containing PHI. With respect to security breaches, the proposed regulations will likely extend liability for breaches to business associates ("Business Associates") and subcontractors, and eliminate or modify the existing safe harbor that allows health care providers to avoid reporting security breaches that have no tangible harm.

B. Enforcement Activity

While the proposed regulations interpreting the Omnibus Rule have remained at OMB, there has been no reduction in enforcement activity at OCR. This is illustrated by the steady stream of settlements coming out of OCR, many of which are among OCR's most notable. These include the following:

1. On September 17, 2012, Massachusetts Eye & Ear Infirmary agreed to pay $1.5 million to settle with OCR. The hospital came under investigation due to a security breach in which an unencrypted laptop containing PHI was stolen. Although any threat to individuals was neutralized by remotely erasing the laptop's hard drive, OCR used the breach notification as an opportunity to investigate the hospital's general HIPAA compliance and found widespread violations. This demonstrates OCR's willingness to leverage breach notifications or other complaints into full-scale audits of an organization's overall privacy practices.

2. In April 2012, Phoenix Cardiac Surgery, P.C., agreed to a $100,000 settlement after OCR discovered that the five-person practice used a publicly viewable Internet calendar for scheduling its patients. This settlement signals that OCR does not intend to focus enforcement solely on hospitals, health plans, and other large Covered Entities. Small organizations, such as physician practices, also are at risk of being investigated and penalized for violating HIPAA.

3. In June 2012, the Alaska Department of Health and Human Services ("DHHS") settled with OCR for $1.7 million. Like Massachusetts Eye and Ear Infirmary, the Alaska DHHS had a small security breach after which OCR

discovered widespread violations of HIPAA in the organization, including a failure at the Alaska DHHS to conduct a security risk assessment, complete appropriate security training, or implement necessary device and media controls. This settlement is notable because it involves a state agency and demonstrates OCR's willingness to pursue enforcement actions outside of the private sector.

The above settlements also are noteworthy because they reveal renewed interest at HHS in enforcing violations of the HIPAA Security Rule, which, for many years, had taken a backseat to Privacy Rule enforcement. For example, in OCR's settlement with Alaska DHHS, many of the violations described in the settlement were Security Rule violations (including the failure to perform a risk assessment, complete security training, and implement necessary device and media controls).

Such concerns about Security Rule compliance also are reflected in OCR's statistics on the most common types of enforcement cases. OCR's current data shows that most of its enforcement cases involve the following three types of violations: (i) theft of data or data storage devices (e.g., USB drives or laptops), (ii) unauthorized access/disclosure of data, and (iii) loss of data or data storage devices. These are the types of violations that typically arise when an organization has failed to implement appropriate security safeguards.

C. Audit Program

In 2012, OCR commenced the pilot phase of the Audit Program. In this pilot phase, OCR has engaged a firm, KPMG, to audit the privacy and security practices of 115 selected Covered Entities. OCR stated that the goals of the Audit Program are to assess compliance efforts and identify best practices and deficiencies. The Phase I audits began in November 2011 and will likely conclude in December 2012. Following the conclusion of the pilot phase, the Audit Program will become permanent and auditors will begin targeting HIPAA Business Associates in addition to Covered Entities. Recently, OCR released preliminary findings from the first round of the Phase I audits. According to these findings, the most common deficiencies identified by KPMG to date include:

- Inadequate patient designations of personal representatives;
- Insufficient documentation justifying a denial of access to records;
- Failure to perform security risk assessments;
- Absent contracts between Covered Entities and Business Associates; and
- Poor plans for timely notification in the event of a security breach.

Although the KPMG audits are revealing a number of deficiencies in the privacy and security practices of HIPAA-regulated entities, OCR has stated that enforcement

investigations are not the goal of the Audit Program. Nonetheless, information obtained through program audits could lead to enforcement actions, and the Audit Program will provide OCR with information on where to direct enforcement and compliance efforts in the future. Common deficiencies, such as those that KPMG identified, may therefore become the basis for future enforcement actions.

D. Other Federal Program Initiatives

There are many other ongoing efforts at HHS aimed at promoting compliance with HIPAA and improving health privacy and security practices, including a number of efforts focused on access to health records. For example, under the newly issued Stage 2 "Meaningful Use" requirements for eligibility in the EHR certification program (released in August of this year but not effective until 2014), certified EHR providers must be able to provide individuals with electronic access to their medical records within four business days of the information being available to the provider. Also, as part of a separate effort, multiple agencies—including the Department of Veterans Affairs, the Department of Defense, and HHS—have instituted "blue button" programs that enable their beneficiaries to download their medical records directly.

E. State Activity

While 2012 was certainly an action-packed year at the federal level, there also were significant developments in several states. The year 2012 saw a HIPAA lawsuit filed by a state attorney general, only the third such lawsuit of its kind. When the HITECH Act was passed in 2009, it authorized state attorneys general to prosecute HIPAA claims and allowed them a share in the penalties recovered. On May 25, 2012, the Massachusetts Attorney General's Office settled a HIPAA claim against South Shore Hospital for $700,000 after it was revealed that the hospital lost boxes of electronic data containing PHI. While HIPAA suits filed by state attorneys general are still infrequent, the shift towards EHRs and the financial gains available to states through the HITECH Act's "bounty sharing" provision suggests that state attorneys general are likely to become more active in their enforcement of HIPAA.

More significantly, the Texas and California Legislatures passed substantial revisions to their privacy statutes in 2012. The Texas Medical Privacy Act ("Act"), which took effect on September 1, 2012, significantly increases the state's privacy protections and enforcement tools. The statute radically expands Texas's breach notification rules. Covered Entities in Texas must now notify affected individuals *even if those individuals reside in states that do not require notification*. The Act also mandates new employee training requirements, imposes steep fines for wrongfully disclosing PHI, and narrows the timeframe for providing individuals with access to their medical records to 15 days, instead of the 30 days required by HIPAA.

In California, by contrast, A.B. 439, which was signed into law on September 22, 2012, provides some relief for Covered Entities and Business Associates subject to California's onerous security breach nominal damages provision. In California, Covered Entities can be forced to pay $1,000 per person in nominal damages in the event of a

security breach. An important legal issue is whether class actions can be pursued in this regard.

Significantly, A.B. 439 creates a limited affirmative defense to the nominal damages provision, exempting Covered Entities and Business Associates if they are able to demonstrate that:

- the entity took reasonable and appropriate corrective action after a disclosure and complied with disclosure notification obligations;
- the entity had preventive security policies and procedures in place; and
- the release of confidential data was solely to another Covered Entity or Business Associate and there is no evidence of medical identity theft.

While this defense is undoubtedly good news for providers operating in California, it is limited to unauthorized disclosures between Covered Entities and Business Associates and would not apply in many cases, where, for example, an entity's data was lost or stolen.

Employers also should be aware of several recent state laws regarding social media in the workplace. Notably, on September 27, 2012, Governor Jerry Brown of California signed A.B. 1844 into law, making California the third state, after Maryland and Illinois, to regulate an employer's access to an employee's social media. The law, which becomes effective on January 1, 2013, prohibits California employers from requesting an employee's or applicant's username or password to social media websites (such as Facebook or a blog), or from requiring an employee to access these social media websites in the employer's presence. However, the law does permit employers to require access from their employees to social media websites when it is necessary for an investigation into the employee's misconduct.

The New Jersey statute, known as "Cathy's Law," was signed by Governor Chris Christie on August 8, 2012. Under Cathy's Law, first responders are forbidden from taking pictures or videos of victims, and from disclosing those images without the victim's consent. Unauthorized posting (which is also a violation of HIPAA) carries a criminal penalty in New Jersey. Notably, Cathy's Law does permit first responders to take images at emergency scenes in accordance with their employers' rules, regulations, or operating procedures. Therefore, employers operating in New Jersey with employees who may be first responders should ensure that their policies for recording accidents comply with this new law.

Conclusion

The regulatory landscape for privacy and security continues to evolve as regulators seek to establish new norms for the handling of health information in the modern information age. In this environment, state and federal regulators are aggressively exercising their enforcement powers and appear willing to use all the tools at their

disposal to promote industry compliance with privacy and security laws. This new order will likely continue throughout 2013. As privacy and security practices of health care companies are increasingly becoming the object of regulatory scrutiny, now more than ever, HIPAA-regulated entities should seriously consider having a review conducted of their privacy and security practices, following up with risk assessments, and taking other steps to ensure that adequate privacy and security programs and safeguards are in place.

* * *

This Client Alert was authored by **Ross K. Friedberg** *and* **Ophir Stemmer**. *For additional information about the issues discussed in this Client Alert, please contact one of the authors or the Epstein Becker Green attorney who regularly handles your legal matters.*

About Epstein Becker Green

Epstein Becker & Green, P.C., founded in 1973, is a national law firm with approximately 300 lawyers practicing in 11 offices, in Atlanta, Boston, Chicago, Houston, Indianapolis, Los Angeles, New York, Newark, San Francisco, Stamford, and Washington, D.C. The firm is uncompromising in its pursuit of legal excellence and client service in its areas of practice: Health Care and Life Sciences, Labor and Employment, Litigation, Corporate Services, and Employee Benefits. Epstein Becker Green was founded to serve the health care industry and has been at the forefront of health care legal developments since 1973. The firm is also proud to be a trusted advisor to clients in the financial services and hospitality industries, among others, representing entities from startups to Fortune 100 companies. Our commitment to these practices and industries reflects the founders' belief in focused proficiency paired with seasoned experience. For more information, visit www.ebglaw.com.

The Epstein Becker Green Client Alert is published by EBG's Health Care and Life Sciences practice to inform health care organizations of all types about significant new legal developments.

Lynn Shapiro Snyder, Esq.
EDITOR

If you would like to be added to our mailing list or need to update your contact information, please contact Kristi Swanson at kswanson@ebglaw.com or 202-861-4186.

ATLANTA
Robert N. Berg
Michael V. Coleman
J. Andrew Lemons
Kenneth G. Menendez
Marisa N. Pins
Evan Rosen
Alan B. Wynne

BOSTON
Barry A. Guryan

CHICAGO
Amy K. Dow
Lisa J. Matyas
Griffin W. Mulcahey
Kevin J. Ryan

HOUSTON
Mark S. Armstrong
Daniel E. Gospin
Pamela D. Tyner

LOS ANGELES
Adam C. Abrahms
Dale E. Bonner
Ted A. Gehring
J. Susan Graham
Kim Tyrrell-Knott

NEW YORK
Nicholas S. Allison
Eric L. Altman
Jeffrey H. Becker
Vinay Bhupathy*
Michelle Capezza
Stephanie Carrington*
Aime Dempsey
Sarah K. diFrancesca
Kenneth W. DiGia
Jerrold I. Ehrlich
Hylan B. Fenster
James S. Frank
Arthur J. Fried
Paul A. Friedman
Philip M. Gassel
Jay E. Gerzog
John F. Gleason
Robert D. Goldstein
Wendy C. Goldstein
Robert S. Groban, Jr.
Gretchen Harders
Jennifer M. Horowitz
Kenneth J. Kelly
Joseph J. Kempf, Jr.
Jane L. Kuesel
Stephanie G. Lerman
Purvi Badiani Maniar
Wendy G. Marcari
Eileen D. Millett
Leah A. Roffman
Tamar R. Rosenberg
William A. Ruskin
Jackie Selby
Catherine F. Silie
Victoria M. Sloan
Steven M. Swirsky
Natasha F. Thoren

NEWARK
Joan A. Disler
James P. Flynn
Daniel R. Levy
Philip D. Mitchell
Maxine Neuhauser
Michael J. Slocum
Sheila A. Woolson

STAMFORD
David S. Poppick

WASHINGTON, DC
Kirsten M. Backstrom
Emily E. Bajcsi
Clifford E. Barnes
James A. Boiani
George B. Breen
Lee Calligaro
Jesse M. Caplan
Jason B. Caron
Jason E. Christ
Eric J. Conn
Tanya V. Cramer
Anjali N.C. Downs
Gregory H. Epstein
Steven B. Epstein
Ross K. Friedberg
Daniel C. Fundakowski*
Brandon C. Ge*
Stuart M. Gerson
David C. Gibbons*
Shawn M. Gilman
Jennifer K. Goodwin
Daniel G. Gottlieb
Philo D. Hall
Douglas A. Hastings
Dawn R. Helak
Robert J. Hudock
William G. Kopit
Jennie B. Krasner
Amy F. Lerman
Christopher M. Locke
Katherine R. Lofft
Julia E. Loyd
Mark E. Lutes
Kara M. Maciel
Benjamin S. Martin
Teresa A. Mason*
David E. Matyas
Colin G. McCulloch
Frank C. Morris, Jr.
Leslie V. Norwalk
Kathleen A. Peterson
Daniela A. Pirvu
René Y. Quashie
Jonah D. Retzinger
Joel C. Rush
Serra J. Schlanger
Deepa B. Selvam
Alaap B. Shah
Lynn Shapiro Snyder
Adam C. Solander
Ophir Stemmer
David B. Tatge
Daly D.E. Temchine
Bradley Merrill Thompson
Carrie Valiant
Dale C. Van Demark
Patricia M. Wagner
Robert E. Wanerman
Constance A. Wilkinson
Kathleen M. Williams
Lesley R. Yeung

**Not Admitted to the Practice of Law*

This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

© 2012 Epstein Becker & Green, P.C.

Attorney Advertising