HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Ten
Number One
January 2008
Published Monthly

12TH ANNUAL COMPLIANCE INSTITUTE

APRIL 13–16, 2008 | NEW ORLEANS, LA
HILTON RIVERSIDE NEW ORLEANS visit www.compliance-institute.org

Meet HCCA's 5,000th Member

Libby Easton-May
Director of Compliance, Operations & Marketing,
WellPoint Senior Business Division
PAGE 14

HIPAA's Privacy Regulations: Appropriate safeguard, unmanageable obstacle, or convenient scapegoat?
PAGE 4

Also:
When worlds collide: Health care compliance and union work force
PAGE 44

Feature Focus:
Review of the OIG Work Plan FY 2008
PAGE 32

HIPAA's Privacy regulations: Appropriate safeguard, unmanageable obstacle, or convenient scapegoat?

By Jeffrey L. Kapp, Esq.

Editor's note: Jeffrey L. Kapp is a partner in the Columbus, OH office of Jones Day. He may be reached by telephone at 614/469-3939 or by e-mail at jlkapp@jonesday.com.

The tragedy at Virginia Tech in April 2007 caused the issue of compliance with the privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to return to public consciousness. In light of the Virginia Tech incident and recent media attention involving episodes of misapplication of HIPAA's privacy regulations[1] (the "Privacy Regulations"), calls from various interested parties regarding the need to revisit the Privacy Regulations are growing. For example, the Report to the President on Issues Raised by the Virginia Tech Tragedy (the "Presidential Report"), prepared by the Secretaries of the U.S. Department of Health and Human Services, the Department of Education, and the Attorney General of the U.S. Department of Justice and issued on June 13, 2007, touched on HIPAA issues. The Presidential Report concluded that

> "States, which have long sought to address the difficult balance among privacy, security and ensuring that people in need receive appropriate care, also report that they may be revisiting their approach in the coming months, as tragic events such as Virginia Tech sharpen their focus on whether the balances that have been struck are correctly calibrated or whether there is a need to implement more effectively decisions that have already been made."

This article will highlight several provisions of the Privacy Regulations that are common areas of complaint or misunderstanding and examine whether the Privacy Regulations are an appropriate safeguard for protected health information (PHI), an unmanageable obstacle to appropriate sharing of PHI, or a convenient scapegoat for covered entities to use in handling requests for PHI. Finally, this article will provide some suggestions for maintaining the delicate balance between patient privacy and appropriate uses and disclosures of PHI in compliance with the Privacy Regulations.

Background

Although it is impossible to condense the Privacy Regulations and the voluminous commentary surrounding the numerous iterations of the Privacy Regulations, the basic premise is that covered entities (e.g., health care providers, health plans, and health care clearinghouses) cannot use or disclose an individual's PHI without the individual's authorization, except for uses and disclosures for the purposes of treatment, payment, and health care operations of the covered entity.

The Privacy Regulations enumerate a number of additional exceptions to the authorization requirements that address specific circumstances under which PHI can be used or disclosed without the individual's authorization (e.g., as required by law, for judicial and administrative proceedings, to avert serious threat to health or safety). Two other important considerations in analyzing and applying the Privacy Regulations are: (1) the Privacy Regulations create a privacy "floor" by creating a minimum level of protection for PHI, and covered entities are free to use more restrictive standards, and (2) the Privacy Regulations permit the uses and disclosures of PHI described above, but generally do not require that covered entities make such uses or disclosures of PHI.

In some instances, the Privacy Regulations grant flexibility by creating standards that require covered entities to take "reasonable" steps or use "professional judgment" in determining when and how much PHI may be used or disclosed. These standards allow for additional flexibility, but they also create confusion, ambiguity, and differing interpretations and understandings of permissible actions under the Privacy Regulations. The Presidential Report found a "consistent theme and broad perception in our meetings… that this confusion and differing interpretations about state and federal privacy laws and regulations impede appropriate information sharing." The result of this confusion and inconsistent interpretation of the Privacy Regulations, coupled with the fear of violating the regulations, have led to conservative interpretations (or misinterpretations) of the requirements. Thus, in many cases, the Privacy Regulations have had the unintended consequence of preventing permitted uses and disclosures of PHI.

"Minimum necessary" standard

The "minimum necessary" standard [set forth at 45 CFR § 164.502(b)] requires that covered entities make reasonable efforts to limit uses and disclosures of, and requests for, PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standard does not apply to several types of uses and disclosures by a health care provider for treatment purposes, those required by law, those made to the individual who is the subject of the PHI, and those made pursuant to a HIPAA-compliant authorization.

The minimum necessary standard is an area of frequent misunderstanding, because some covered entities do not realize that these exceptions exist. For example, if a physician requests a patient's file from a hospital's medical record department, the Privacy Regulations permit the hospital to send a copy of the entire medical record to the physician. Some facilities have reported that unless a provider requests the entire medical record, the facility will disclose only a default level of treatment information (e.g., discharge summary, history and physical, lab results from the past several days). While this approach is permissible under the Privacy Regulations (the Privacy Regulations do not mandate a disclosure of all PHI) and may reduce some upfront costs, it may not always be in the best interest of the facility. Incomplete disclosures may lead to relatively minor inconveniences, such as processing additional requests for information, or could lead to major problems, such as missed diagnoses caused by the lack of full disclosure. From an efficiency and cost perspective, incomplete disclosures can also lead to waste due to duplicative diagnostic tests.

From a HIPAA compliance perspective, the minimum necessary standard provides an appropriate safeguard and should not be viewed as an unmanageable obstacle. The Privacy Regulations create exceptions to the minimum necessary standard that allow PHI

What questions should a health care worker ask of someone who inquires about a patient's condition? What if the inquiring person is a relative or close personal friend of the patient? What if the patient is unconscious?

It depends on level of information that will be disclosed. Under HIPAA, covered entities are permitted to use a facility directory to inform visitors or callers about a patient's location in the facility and general condition. HIPAA's privacy regulations permit covered entities to maintain a directory of certain types of information about patients, such as patient name, location in the facility, health condition expressed in general terms that does not communicate specific medical information about the individual, and religious affiliation. If the patient has not opted out being included in the directory after proper explanation from the covered entity, the health care worker can disclose the directory information to any person making an inquiry. If, due to emergency or incapacity, the patient has not been provided an opportunity to choose whether his/her directory information may be made available, the directory information about the patient may still be made available if doing so is in the individual's best interest as determined in the professional judgment of the covered entity, and would not be inconsistent with any known preference previously expressed by the individual. The covered entity must inform the patient about the directory and provide the patient an opportunity to make a choice regarding disclosures as soon as practicable after the emergency event or incapacity has subsided.

Further, HIPAA's privacy regulations permit covered entities to disclose to a family member, relative, or close personal friend of the individual, the protected health information that is directly relevant to that person's involvement with the individual's care or payment for care. These types of disclosures may also be made to persons who are not family members, relatives, or close personal friends of the individual, if the covered entity has reasonable assurance that the person to whom the disclosures are made has been identified by the individual as being involved in his or her care or payment. Note, if the individual is present, this type of disclosure may only be made if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure. If the individual is not present or is incapacitated, the covered entity may make the disclosure if, in the exercise of its professional judgment, it believes the disclosure is in the best interests of the individual. As with all privacy questions, because HIPAA's privacy regulations are a privacy "floor" that provides minimum protection, health care workers should consult their organization's applicable policies and procedures to ensure that their organization does not set a higher threshold (either by reason of organizational beliefs or applicable state law).

Can a covered entity disclose a patient's status as "treated and released" or deceased as part of a release of directory information?

Yes, if that a patient has not opted out of the directory and the covered entity has followed the appropriate HIPAA requirements regarding directories, a covered entity may disclose that a patient has been "treated and released" or died.

to be disclosed without applying the minimum necessary standard. Further, when the minimum necessary standard applies, covered entities should already have in place policies and procedures that guide personnel on how to take reasonable efforts to determine the appropriate amount of PHI to be used or disclosed in a particular situation. Because of the flexibility afforded by the minimum necessary standard, covered entities should be careful in using the Privacy Regulations as the reason for failing to disclose PHI, especially in response to a treatment-related request. That said, HIPAA does not prevent covered entities from establishing their own standards for disclosures, as long as the self-imposed standard is more restrictive than the Privacy Regulations' standard.

Disclosures to family members

Another area of HIPAA concern is the disclosure of health information to family members. The Privacy Regulations allow covered entities to disclose to a family member, other relative, close personal friend, or any other person identified by the individual, the PHI "directly relevant to such person's involvement with the individual's care or payment related to the individual's health care." [45 CFR § 164.510(b)]. Covered entities may disclose this information if the individual agrees or does not object, or if the covered entity "reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure." The covered entity can make a disclosure based upon this reasonable inference, even if the individual is not present.

Not surprisingly, covered entities are constantly bombarded with information requests for patient information from patients' family members. These requests put covered entities in a difficult position. On one hand, covered entities are sympathetic to family members who want and/or need to know the health information about their loved ones. Further, providing information to appropriate representatives of a patient can be beneficial to the patient and to the provider's ability to deliver care. On the other hand, allegedly improper disclosures of PHI to family members are a common cause of patient privacy complaints. Therefore, covered entities are forced to balance these competing interests, often in emotionally-charged settings. Choosing not to disclose information to family members is a convenient default position to take, because it involves less risk and it is easy to use HIPAA as the excuse for not disclosing information. However, relying on this default position may cause a covered entity to be perceived negatively by dissatisfied patients and families and may give the appearance that the covered entity does not understand the Privacy Regulations.

From a compliance perspective, three components of this standard are of particular importance.

First, if possible, the individual should be given the opportunity to identify the people to whom the covered entity may disclose the individual's PHI. The process of providing this opportunity need not be overly burdensome on the covered entity (documented verbal communications would be sufficient) and provides the covered entity with additional assurance of compliance.

Second, the disclosure of information to the family member (or other person) needs to be "directly relevant" to the family member's involvement in the individual's care or payment for such care. This component allows covered entities some leeway in determining the type and amount of PHI that is directly relevant. Although this component provides flexibility, covered entities need to ensure that these determinations are made in a consistent manner and in accordance with the covered entity's policies and procedures.

Third, although the safest course is to obtain a patient's consent, the Privacy Regulations allow disclosures to family members (and certain other people) if the covered entity reasonably infers, using professional judgment, that the individual does not object. This component should provide comfort to covered entities, because the standard is not whether they are correct in their inference that disclosure would be permissible, rather the standard is whether the covered entity used reasonable professional judgment in reaching its conclusion. As with minimum necessary standard, the Privacy Regulations provide an appropriate safeguard of PHI for the individual and provide flexibility to the covered entity in determining when a disclosure may be made. This standard should not act as an unmanageable obstacle to PHI disclosure to appropriate family members at appropriate times.

Averting a serious threat to health or safety

The Privacy Regulations permit covered entities to disclose PHI, consistent with applicable law and standards of ethical conduct, if the covered entity has a good faith belief that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. [45 CFR § 164.512(j)] Covered entities must make this disclosure to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. However, the Privacy Regulations do not permit use or disclosure of PHI if the covered entity learns the information (a) in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure or (b) through a request by the individual to initiate or to be referred for the treatment,

Continued on page 8

counseling, or therapy regarding such propensity. A covered entity that uses or discloses PHI pursuant this exception is presumed to have acted in good faith, if the covered entity's belief regarding the threat is based upon the covered entity's actual knowledge or upon a credible representation by a person with apparent knowledge or authority.

The occurrence of events that necessitate using the exception for averting a serious threat to health or safety is less frequent than the other occurrences described in this article, but the stakes are considerably higher. Recent events highlight the importance of a covered entity's ability to rapidly address potential threats to individuals or to the general public's safety. Covered entities need to be prepared to address the issue quickly and weigh the risks of disclosure against the probability and magnitude of potential harm. Misunderstandings concerning the flexibility afforded by this exception likely arise because covered entities do not handle these types of threats regularly and, when such threats do occur, the circumstances surrounding the event make it difficult for the covered entity to respond calmly and quickly.

Covered entities' compliance efforts should focus on identifying potential threats and being prepared to address them. Because these threats arise unexpectedly and need immediate resolution, it is important that policies and procedures (including specific examples) be in place and be readily accessible, if such a situation arises. These policies and procedures need to consider not only the Privacy Regulations concerns, but also address professional and ethical requirements that might restrain or allow disclosure of patient information.

Finally, the decision of whether or not to disclose PHI in this situation should be escalated rapidly to an individual in the organization who is responsible for privacy compliance. This type of disclosure (or decision not to disclose) could have a significant impact on the covered entity and the community that it serves. If applied reasonably, this provision of the Privacy Regulations should adequately safeguard patient information while meeting the obvious public policy interest of preventing harm to other individuals. The presumption of good faith granted to covered entities with respect to this type of disclosure makes the decision of whether or not to disclose PHI more manageable and significantly lessens a covered entity's ability to blame HIPAA for a failure to disclose PHI in the face of serious threat. When possible, covered entities should document the process undertaken in making its determination of whether or not to disclose PHI in response to a potential threat.

Lessons

Covered entities (or more accurately, employees of covered entities) will continue to misapply the Privacy Regulations, both unintentionally and intentionally, unless personnel are properly trained to decide when, to whom, and how much PHI is disclosed. This training should include educating personnel to know when matters should be taken to the organization's HIPAA experts in the Compliance or Legal departments. Covered entities also need to examine their own policies and procedures to determine when (or if) there are situations when internal policies are more restrictive than the Privacy Regulations for PHI disclosures. If the policies and procedures are stricter than the Privacy Regulations, the covered entity should confirm that the additional restriction is intentional and justifiable.

Covered entities should consistently apply their privacy policies and procedures, because decisions involving the use or disclosure of PHI impact patient and customer satisfaction, as well as the covered entities' reputation. Using the Privacy Regulations as an excuse to avoid disclosing PHI is a strategy that is not without cost. In addition to the loss of patient satisfaction and trust on an

How much can a nurse tell a police officer about a suspected case of child abuse or vulnerable elder abuse? At what point can he/she disclose it?

Under HIPAA, child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports. In these cases, the agreement of the individual is not required and the minimum necessary standard does not apply. Therefore, sound professional judgment and common sense will dictate when a disclosure should be made.

Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such reports if the nurse reasonably believes the individual to be a victim of abuse, neglect or domestic violence and if (a)the individual agrees, (b) the report is required by law and the disclosure is limited to the relevant requirements of the law; (c) the disclosure is expressly authorized by law and, based on the exercise of nurse's professional judgment, the report is necessary to prevent serious harm to the individual or others, or (d) the disclosure is expressly authorized by law and certain other exigent circumstances exist.

Because of the complexities involved in these types of cases, it is best for employees of covered entities to consult with the Privacy Officer to ensure that the proper disclosures are made to the appropriate parties in an efficient and legally-compliant manner.

individual basis, an organization could face the wrath of an entire community. The Report of the Virginia Tech Review Panel to the Governor of the Commonwealth of Virginia was quite direct in its criticism of this approach:

> "Privacy laws can block some attempts to share information, but even more often may cause holders of such information to default to the nondisclosure option – even when laws permit the option to disclose. Sometimes this is done out of ignorance of the law, and sometimes intentionally because it serves the purposes of the individual or organization to hide behind the privacy law. A narrow interpretation of the law is the least risky course, notwithstanding the harm that may be done to others if information is not shared."[2]

Covered entities should resist the temptation to make HIPAA the scapegoat for choosing not to disclose PHI because, depending on the situation, such a response may no longer be tolerated by patients or the general public.

The views set forth herein are the personal views of the author and do not reflect those of the Jones Day law firm.

1. See, e.g., "Keeping Patients' Details Private, Even from Kin," The New York Times, July 3, 2007, Jane Gross.
2. Report of the Review Panel Presented to Governor Kaine, Commonwealth of Virginia, August 2007, p. 63. Available at http://www.vtreviewpanel.org/. Accessed October 11, 2007.

Be Sure to Get Your CHC CEUs

Inserted in this issue of **Compliance Today** is a quiz related to this article: "HIPAA's Privacy Regulations: Appropriate safeguard, unmanageable obstacle, or convenient scapegoat?" by Jeffrey L. Kapp beginning on page 4.

To obtain your CEUs, take the quiz and print your name at the top of the form. Fax it to Liz Hergert at 952/988-0146, or mail it to Liz's attention at HCCA, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Questions? Please call Liz Hergert at 888/580-8373.

Compliance Today readers taking the CEU quiz have ONE YEAR from the published date of the CEU article to submit their completed quiz.

CHC CERTIFIED IN HEALTHCARE COMPLIANCE

The Compliance Professional's Certification

The Healthcare Compliance Certification Board (HCCB) compliance certification examination is available in all 50 states. Join your peers and become Certified in Healthcare Compliance (CHC).

CHC certification benefits:

- Enhances the credibility of the compliance practitioner
- Enhances the credibility of the compliance programs staffed by these certified professionals
- Assures that each certified compliance practitioner has the broad knowledge base necessary to perform the compliance function
- Establishes professional standards and status for compliance professionals
- Facilitates compliance work for compliance practitioners in dealing with other professionals in the industry, such as physicians and attorneys
- Demonstrates the hard work and dedication necessary to perform the compliance task

Since June 26, 2000, when CHC certification became available, hundreds of your colleagues have become Certified in Healthcare Compliance. Linda Wolverton, CHC, says she sought CHC certification because "many knowledgeable people work in compliance and I wanted my peers to recognize me as one of their own."

For more information about CHC certification, please call 888/580-8373, e-mail hccb@hcca-info.org or click on the HCCB Certification button on the HCCA Web site at *www.hcca-info.org*.

Congratulations on achieving CHC status! The Health Care Compliance Certification Board announces that the following individuals have recently successfully completed the Certified in Healthcare Compliance (CHC) examination, earning CHC designation:

Linda Betts
Cecelia L. Bishop
Steve Brodie
T Richard Bruan
Ann Chaglassian
Christina C. Davis
Linda J. Dietsch
Carey G. Duszak
Royce D. Harrell
Lorene M. Hartmann
Kimberly Marie Hrehor
Jan M. Jameson
Cathy Denise Johnson
Kathleen M. Kahler
John Kelley
Jeffrey P. Mastej
Judith L. Miller
Rosa Lynn Moody
Debora A. Murray
Annette Divers Norton
Jennifer Miller O'Brien
Felix O. Okhiria
Sara Susann Powers
Chandrika Raghavan
Terry L. Reeves
Maria L. Rivera
Kimberly H. Rizzo
Jeannette A. Schuler
Marjorie Jean Scott
Rebecca A. Sherlock
Matthew F. Tormey
Madeleine Anne Williams