These materials were produced using federal emergency preparedness and response grant funding while Mr. Gravely was a partner at another firm.

Neither that firm, nor Gravely Group, can assert ownership of these materials since they were paid for with federal grant funds.

Gravely Group is making these materials available to the public, without charge, in response to the national public health emergency caused by the novel coronavirus.

Gravely Group hopes that these materials are helpful. If you choose to use them, we do request that you provide attribution to Steve Gravely.

Sharing Information During Disasters: HIPAA Implications

Prepared by:
Steve Gravely, J.D., M.H.A.
Erin Whaley, J.D., M.A.

April 23, 2007

Table of Contents

Introduction

Preparations for mass casualty events, including an influenza pandemic, have caused health care providers to question whether the privacy protections of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") will inhibit their ability to respond. While health care providers will need to share PHI with other entities during any large scale disaster or emergency for various reasons, this need will be particularly important in a public health emergency. Hospitals must understand the contours and nuances of their responsibilities under HIPAA during disasters as well as ways in which they can protect themselves from liability for potentially unavoidable violations. For instance, there are a variety of emerging initiatives such as patient tracking, absence reporting, and employee screening programs, which are being developed to enhance health care providers' responses to disasters. While none of these initiatives are expressly prohibited by HIPAA, consideration must be given to protecting the PHI that may be used and disclosed with these initiatives.

This paper focuses generally on those disclosures permitted by HIPAA which will be most relevant during disasters: (1) for treatment, payment and operations; (2) required by law; (3) for public health activities; (4) to avert a serious threat to health or safety; (5) for national security and intelligence activities, and; (6) to notify those involved in the individual's health care.[1]

The results of this analysis are mixed. The good news is that, during an emergency or disaster, there are numerous regulatory exceptions to HIPAA that will permit hospitals to share protected health information with other providers, public health authorities and certain other designated parties. The bad news is that, even during a disaster, the majority of HIPAA

[1] *See* U.S. Department of Health and Human Services Office for Civil Right, "Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situation," September 2, 2005 (Bulletin #1) for a brief overview of permissible disclosures of PHI in emergency situations.

requirements will remain in effect so hospitals must plan as if they will be responsible for fulfilling all HIPAA obligations even in the midst of a disaster.

I. Overview of HIPAA

Passed by Congress in 1996, HIPAA created a new "civil right" for the protection of personally identifiable health information.[2] The Privacy provisions of HIPAA were significantly delayed in their implementation and the final Privacy Rule was not effective until 2001.[3] Once effective, HIPAA imposed sweeping new restrictions on how PHI is used and disclosed by covered entities. In anticipation of the Privacy Rules becoming final, health care providers implemented comprehensive new policies and procedures to comply with HIPAA and spent countless hours educating their staff on HIPAA requirements. There were widespread concerns that HIPAA would prevent hospitals from functioning and that the burden of HIPAA compliance would inhibit the delivery of care. These concerns have not materialized in terms of the daily operation of health care facilities, but still exist when contemplating a hospital's response to a wide scale emergency or disaster. While extensive guidance has been issued in recent years clarifying HIPAA's privacy rules in both everyday and disaster circumstances, HIPAA compliance remains an extremely important and often complex issue for health care providers.

At its core, HIPAA regulates the use and disclosure of "protected health information" (PHI) by "covered entities," which includes hospitals and other health care providers. Protected Health Information is very broadly defined to include all individually identifiable health information that relates to a past, present or future physical or mental health condition of an individual, the provision

[2] Pub. L. 104-191

[3] The final Privacy Rule became effective April 14, 2001 with compliance required by April 14, 2003. See http://www.hhs.gov/ocr/hipaa/bkgrnd.html for more information.

of health care to an individual, or payment for care.[4] For HIPAA purposes, "use" generally refers to the ways in which PHI is used within a HIPAA Covered Entity. "Disclosure" refers to the sharing of PHI by a Covered Entity with others.

"A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request."[5] Whether or not the "minimum necessary" standard applies to a given use or disclosure is a function of the regulatory requirements surrounding that use or disclosure. Applicability of the standard will be discussed in the context of each permissive use discussed in this paper.

In addition to abiding by the "minimum necessary" rule when applicable, patient consent or authorization is required for virtually all uses and disclosures of PHI. "Consent" under HIPAA requires that the patient be informed of his privacy rights through a Notice of Privacy Practices and be allowed to set some limitations on how his PHI can be shared. Fortunately for health care providers, HIPAA does allow for consents to be rather generally worded to cover all uses and disclosures related to treatment, payment and health care operations, and to remain in effect until revoked. These general consents allow providers to use and disclose a patient's PHI, as necessary and subject to other HIPAA restraints, without having to obtain additional consents from the patient. These consent provisions have been incorporated into hospital operations.

A covered entity must obtain the individual's written "authorization" for any use or disclosure of protected health information that is not for treatment, payment or health care

[4] 45 C.F.R. § 160.103

[5] 45 C.F.R. § § 164.502(b) and 164.514(d).

operations or otherwise permitted or required by the Privacy Rule.[6] "Authorization" under HIPAA is very different from "consent." As opposed to the general nature of consents, in an authorization, a patient gives permission for the covered entity to use or disclosure his PHI for a certain purpose or limited event. Such authorizations must be treated as part of the medical record and the covered entity must keep a record of the information that was disclosed pursuant to the authorization.

Outside of this framework, "[t]he Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[7] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information."[8] It is a subset of these 12 national priority purposes that will be the focus of this paper as, outside of treatment, they will be the most relevant to information sharing during a disaster.

It is important for covered entities to understand the nuances, contours and requirements of HIPAA because failure to comply can result in investigations and penalties. HIPAA enforcement is a compliant driven process that is managed by the Office of Civil Rights ("OCR"). OCR does not initiate investigations of a covered entity's compliance absent a complaint. OCR has stated that it will make every effort to counsel providers on how to improve compliance with HIPAA provisions. This has provided some reassurance that enforcement will be even-handed

[6] 45 C.F.R. § 164.508.

[7] *See* 45 C.F.R. § 164.512.

[8] OCR Privacy Brief, "Summary of the HIPAA Privacy Rule," available at http://www.hhs.gov/ocr/privacysummary.pdf (last visited March 23, 2007) (the "OCR Summary").

and conducted in a way to help effective compliance by the covered entity. However, responding to a HIPAA complaint can be extremely time consuming and difficult.

In addition to the stress associated with the investigation of a HIPAA compliant, if a violation is found, the covered entity can be subjected to civil and/or criminal penalties depending on the facts surrounding the violation.[9]

III. OCR Tool for Sharing PHI During Disasters

The U.S. Department of Health and Human Services Office of Civil Rights ("OCR") recently issued a HIPAA emergency planning tool.[10] This tool, which is essentially a flowchart that healthcare providers can use to determine whether they are permitted to share information during a public health emergency, was designed to yield quick answers for the provider. "The tool focuses on the source of the information being disclosed, to whom the information is being disclosed, and the purposes of the information being disclosed."[11] While this tool can yield rapid answers, it cannot answer the

The OCR HIPAA decision tool is available at http://www.hhs.gov/ocr/hipaa/decisiontool.

[9] "HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement. Pub. L. 104-191; 42 U.S.C. § 1320d-5 That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

"A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment. Pub. L. 104-191; 42 U.S.C. § 1320d-6. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice." The OCR Summary.

[10] *See* U.S. Department of Health and Human Services Office for Civil Rights, "HIPAA Privacy Rule: Disclosures for Emergency Preparedness – *A Decision Tool*," *available at* http://www.hhs.gov/ocr/hipaa/decisiontool (last visited August 15, 2006) (the "OCR Tool").

[11] *See* the OCR Tool.

complicated, nuanced HIPAA questions that hospitals will likely have during a public health emergency. Hospitals must still have a thorough understanding of HIPAA's requirements and exceptions in relation to emergencies and disasters.

IV. Treatment, Payment or Health Care Operations

In all situations, including emergencies and disasters, health care providers are allowed to share protected health information ("PHI") as necessary to carry out treatment, payment or health care operations.[12] With the patent consents that health care providers routinely obtain, as described in the Hurricane Katrina Bulletin issued on September 2, 2005 by the Department of Health and Human Services Office for Civil Rights ("Bulletin #1"), treatment includes:

- Sharing information with other providers (including hospitals and clinics),
- Referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
- Coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).

This Bulletin #1 excerpt reflects the fact that, especially during a disaster, OCR will take a fairly broad view of "treatment," which should facilitate the prompt sharing of PHI during emergencies.

When sharing PHI for treatment, "minimum necessary" does not apply.

Where a covered entity is disclosing PHI to another health care provider for treatment purposes, the "minimum necessary" standard does not apply.[13] Where the disclosure is to another person or agency that will use or disclose the information for treatment, however, the minimum necessary standard does apply.[14] For instance, when a hospital

[12] 45 CFR §§ 164.502(a)(1)(ii) and 164.506(c).

[13] *See* 45 CFR § § 164.502(b)(1)(i) and 164.514(d).

[14] 45 CFR § 164.502(b)(1). *See also* the OCR Tool.

discloses PHI to a third party organization that will coordinate patient care, the hospital may only disclose the minimum necessary amount of PHI to accomplish the coordination. Additionally, when disclosures are made for treatment purposes, the accounting requirements are inapplicable because these disclosures are covered by the patient's initial consent.[15]

V. Disclosures Not Related to TPO

Beyond disclosures for payment, treatment and operations, HIPAA does contain strict prohibitions on the disclosure of PHI. However, it also contains numerous exceptions that allow covered entities to share such information without an individual's consent. These exceptions, where applicable, do not turn on the presence or absence of emergency or disaster. Instead, each exception has its own criteria which must be met before it can be used to justify a disclosure without consent. Only those exceptions which may be most relevant during emergencies and disasters are examined, in this paper, specifically those disclosures that are: (1) required by law; (2) for public health activities; (3) to avert a serious threat to health or safety; (4) for national security and intelligence activities, and; (5) to notify those involved in the individual's health care.[16]

Outside of TPO, when an exception applies, PHI can be disclosed without consent.

Required by Law

The HIPAA Privacy Rule allows health care providers to disclose PHI to the extent that such disclosure is required by law.[17] While there are many instances in which a covered entity

[15] 45 CFR § 164.528(a)(1)(i).

[16] *See* U.S. Department of Health and Human Services Office for Civil Right, "Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situation," September 2, 2005 (Bulletin #1) for a brief overview of permissible disclosures of PHI in emergency situations.

[17] 45 CFR § 164.512(a).

will be required to disclose PHI to be compliant with laws (i.e. responding to a subpoena, reporting child abuse), this is a particularly important exception in the communicable disease context. Each state, including Virginia, has a list of "reportable diseases," those diseases which must be reported by health care providers to local health departments. Importantly, according to Virginia's Reportable Disease List, the following diseases must be reported within 24 hours of suspected or confirmed diagnosis by the most rapid means available:

- Disease caused by an agent that may have been used as a weapon;
- All outbreaks;
- Severe Acute Respiratory Syndrome; and
- Unusual occurrence of disease of public health concern.[18]

In Virginia, influenza is a reportable disease.

In addition to these broad categories of diseases which must be reported to the state within 24 hours of suspected or confirmed diagnosis, cases of influenza must be reported to the state within three days of suspected or confirmed diagnosis by laboratory directors, physicians and medical care facility directors.[19] Providers are asked to report the aggregate number of influenza cases each week and the type of influenza if known. Taken together, the list of reportable diseases in Virginia should be broad enough to trigger the "required by law" exception thus enabling hospitals to report any diseases that might lead to a public health emergency.

[18] This is not a comprehensive list of the diseases included on the Virginia Reportable Disease List. For the full list see Virginia Reportable Disease List available at www.vdh.state.va.us/epi/list.asp (last visited August 15, 2006).

[19] Id.

While the minimum necessary standard is not applicable to disclosures that are required by law,[20] covered entities are advised to limit disclosures to the PHI "necessary to meet the requirements of the law that compels the disclosures."[21] Further, when an individual requests an accounting, disclosures made as required by law must be listed.

Public Health Activities

The HIPAA Privacy Rule permits health care providers to disclose PHI to certain recipients for public health activities.[22] Under this exception, covered entities may disclose PHI to "public health authorities" for certain enumerated purposes. The HIPAA regulations define "public health authorities" as (i) those agencies of the federal or state government that are responsible for public health matters as a part of its official mandate; or (ii) any person or entity "acting under a grant of authority from or contract with such" agency.[23]

A covered entity may disclose PHI to a "public health authority that is authorized by law[24] to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, including, but not limited to, the reporting of disease … and the conduct of public

[20] 45 CFR § 164.502(b)(2)(iv).

[21] 65 FR 82525 (December 28, 2000).

[22] 45 CFR § 164.512(b).

[23] 45 CFR § 164.501.

[24] In Virginia, the Commissioner of the Department of Health or his designee is authorized by law to "examine and review any medical records … in the course of investigation, research or studies of diseases or deaths of public health importance." Va. Code Ann § 32.1-40. "Diseases of public health importance" is not a defined term in the Code; therefore, it is unclear under exactly what circumstances the Commissioner can review records. The statute does, however, state that "[n]o such practitioner or person shall be liable in any action at law for permitting such examination and review." Based on this, hospitals should share PHI with the Commissioner, or his designee, when requested for purposes of investigation, research or studies.

health surveillance, public health investigations and public health interventions."[25] Examples of public health authorities covered by this HIPAA provision include local health departments, state public health agencies and federal public health agencies, such as the Centers for Disease Control and Prevention.[26] This exception, therefore, gives health care providers the ability to report communicable disease incidences to local or state health departments so that they may begin or continue surveillance, investigations or interventions.

A covered entity may disclose PHI to a public health authority for:
- ***Surveillance***
- ***Investigations***
- ***Interventions***

It is not clear whether this exception gives covered entities the ability to report PHI to Regional Hospital Coordinating Centers ("RHCC"), local Emergency Operations Centers ("EOC") or the Medical Control Officer ("MCO") for surveillance, investigations or interventions. While these three bodies will play an important role in emergency and disaster preparedness and response, it is not clear that they are "authorized by law" to conduct the enumerated public health activities. Unless there is a statute, regulation, or ordinance authorizing such activities, covered entities probably should not rely on the HIPAA public health activity exception to report PHI to the RHCC, EOC or MCO.

It is not clear that RHCCs, EOCs, and MCOs qualify for the public health exception.

If the public health activities exception does apply, hospitals must remember that they are only able to make disclosures to public health authorities subject to the minimum necessary standards.[27] Covered entities may reasonably rely on a public official's request as constituting

[25] 45 CFR § 164.512(b)(1)(i).

[26] *See* OCR Tool.

[27] *See* 45 CFR § § 164.502(b) and 164.514(d).

minimum necessary for the stated purpose if the public official states that the information requested is the minimum necessary to accomplish the activity.[28]

If informing a person of a potential exposure, do not inform him of the source of the exposure.

A covered entity may also notify individuals who may have been exposed to a communicable disease or who might be at risk of contracting or spreading a disease, when authorized by law in the course of a public health intervention or investigation.[29] Importantly, this exception does not give a covered entity *carte blanche* with respect to informing individuals that they may have been exposed to a communicable disease. The entity may so inform the individual, but not reveal another individual's PHI unless *authorized by law in the course of the public health investigation*. To date, there are no laws in Virginia that authorize a health care provider to make such a disclosure. When informing an individual that he may have been exposed to a communicable disease, therefore, inform him of the potential exposure, the disease in question (if known) and any suggested follow-up care. A health care provider should not reveal the identity of the individual responsible for the exposure unless it has the individual's authorization to do so.

Because employers are understandably concerned about the health and safety of their workforce, covered entities may disclose an employee's PHI to an employer under certain conditions. To qualify for the exception, five criteria must be met:

1. The health care provider provides care to an individual at the request of the employer or the provider is a member of the employer's workforce;
2. The care is being provided to conduct medical surveillance of the workplace or to evaluate work-related illness or injury;
3. The PHI to be disclosed consists of findings concerning work-related illness or injury or a workplace-related medical surveillance;

[28] *See* 45 CFR § 164.514(d)(3)(iii)(A) and the OCR Tool.

[29] 45 CFR § 164.512(b)(1)(iv).

4. The employer needs such findings to comply with the Occupational Safety and Health Administration Act ("OSHA") or the Mine Safety and Health Administration Act ("MSHA"); and
5. The covered provider gives the employee (patient) written notice that PHI will be disclosed to the employer.[30]

In most cases, the limiting factor will be criteria #4, whether the employer needs such findings to comply with OSHA or MSHA. Under the OSHA "general duty clause," employers have a duty to provide their employees with a workplace free from recognized hazards likely to cause death or serious physical harm.[31] Employers have come to appreciate that this means taking certain precautions to help prevent employees from coming in contact with biological hazards, including a pandemic influenza virus, while at work. As part of employers' pandemic preparedness plans, many are considering instituting medical surveillance to quickly identify and contain those employees who have been in contact with the pandemic virus or who are beginning to exhibit symptoms. PHI obtained through this surveillance can likely be released to the employer if the other four requirements are met.

OSHA "General Duty" Clause requires employers to provide a workplace free from hazards.

Outside of a pandemic surveillance context, to comply with OSHA, employers must record all new cases of work-related fatalities, injuries, and illnesses if they involve a number of things, including days away from work, medical treatment, a significant injury or illness diagnosed by a physician, or death.[32] Because most communicable diseases will result in one of these responses, if an employee was infected with a communicable disease through work-related activities, the

[30] 45 CFR § 164.512(b)(1)(v).

[31] See Section 5(a)(1) of the Occupational Safety and Health Act (29 U.S.C. § 654).

[32] 29 CFR § 1904 et seq.

provider rendered treatment at the request of the employer and the other criteria are satisfied, PHI related to the illness can be disclosed to the employer.

Individuals have a right to receive an accounting of all disclosures of PHI made for public health activities.[33] This means that when a covered entity makes a disclosure for public health activities, it must record the date of the disclosure, the name of the entity or person who received the information, the address of the recipient if known, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure.[34] Importantly, this accounting requirement has not been waived in any of the guidance on emergency preparedness and response in relation to HIPAA.

Providers must include disclosures for public health activities in an accounting.

Recognizing that public health authorities may request PHI on a large number of individuals, DHHS has clarified that the Privacy Rule does not require a notation in each medical record that has been accessed by public health authorities.[35] The covered entity need only document the identity (and address if known) of the public health authority to which access was provided, a description of the records and PHI subject to access, the purpose for the disclosure, and when access was provided. This information should be provided to an individual who requests an accounting if the individual's PHI was within the universe of disclosed records. DHHS provides the following example: On August 1, 2003, a hospital began providing a public health authority ongoing access to the medical records of all patients treated in the hospital emergency department to identify reportable cases and extract relevant information required for a particular

[33] 45 CFR § 164.528(a).

[34] 45 CFR § 164.528(b).

[35] *See* http://www.hhs.gov/hipaafaq/permitted/research/465.html, Answer ID 465 (last visited April 23, 2007).

surveillance activity. It would satisfy the HIPAA Privacy Rule to include the following in the accounting:

- the identity and address, if known, of the public health authority;
- a statement that the public health authority had access to medical records for patients treated in its emergency department;
- the date (or approximate range of dates) when the individual's record was subject to access; and
- a statement of the purpose of the access (i.e., identification of the particular public health surveillance activity).[36]

Disclosure of PHI is permitted to abate a serious or imminent threat to the public.

The same basic statement could then be provided in response to a request for an accounting by any individual who was seen in the ED on or after August 1, 2003.[37]

Averting a Threat to Health or Safety

A covered entity may disclose PHI without patient consent to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[38] Disclosure of PHI in such a situation must be to a person or persons reasonably able to abate the threat.[39] For example, when a provider identifies an unexplained disease outbreak suspected to be the result of a bioterrorist attack, the provider may disclose PHI of infected individuals to certain public officials to control the outbreak and prevent further infection.[40] Such disclosures must also comply with the minimum necessary standard[41] and accounting requirements.[42]

---

[36] *Id.*

[37] *Id.*

[38] 45 CFR § 164.512(j). This provision in the HIPAA Privacy Rule is consistent with Virginia law (*see* Va. Code §§ 32.1-127.1:03(D)(6), 32.1-127.1:04).

[39] 45 CFR § 164.512(j)(1)(i)(B).

[40] This course of action may also fall under the public health activities exception.

[41] *See* 45 CFR § § 164.502(b) and 164.514(d).

[42] *See* 45 CFR § 164.528.

Importantly, the Privacy Rule imparts a good faith requirement on the provider disclosing the PHI.[43] There is a presumption that the provider has acted in good faith if its belief in the threat to health or safety is based on actual knowledge or reliance on credible representation by a person with apparent knowledge or authority.[44] The presumption of good faith may shield a provider from liability if a disclosure is made but, in fact, no threat to health or safety is found to exist. In order to overcome the good faith presumption, it would be necessary to prove that the disclosing provider did not base its belief in the threat on actual knowledge or reasonable reliance on a person with apparent knowledge or authority.

There are various exceptions related to notifications.

National Security

Under the HIPAA Privacy Rule, a provider may disclose PHI without patient consent to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities authorized by the National Security Act.[45] This exception may be applicable in a bioterrorist attack situation and would allow providers to disclose PHI to government authorities in the course of their investigation of bioterrorism. While covered entities should keep records on disclosures made pursuant to this exception, individuals do not have a right to receive an accounting of these disclosures.[46]

Notification

In a disaster or emergency, health care providers may disclose the minimum necessary PHI to identify, locate and notify family members, guardians or anyone else responsible for the care of

[43] 45 CFR § 164.528(j)(4)

[44] 45 CFR § 164.512(j)(4).

[45] 45 CFR § 164.512(k)(2); s*ee also* 50 U.S.C. § 401 *et seq*.

[46] 45 CFR § 164.528(a)(1)(iv).

the individual, of the individual's location, general condition or death.[47] Disclosure may be made directly to those involved in the individual's care, the police, the press, the public at large, or to a public or private entity authorized by law or its charter to assist in disaster relief efforts, such as the American Red Cross.[48] Whenever possible, verbal permission to disclose PHI should be obtained from the individual receiving care, but if the person is incapacitated, not available or the permission cannot practicably be provided because of the emergency circumstances, providers may disclose PHI if, in their professional judgment, doing so is in the patient's best interest.[49] Additionally, if obtaining a patient's consent to release information to a disaster relief organization would interfere with the organization's ability to respond to the emergency, such consent is unnecessary.[50]

Similarly, covered entities may use a patient's name, location in the facility, and information about his general condition in the facility directory.[51] While individuals are usually given the opportunity to opt-out of inclusion in the directory, when emergency circumstances make the opportunity to opt-out impractical, such opportunity does not have to be provided.[52] The individual's information can then be included in the directory if the health care provider determines that

Hospitals can have a facility directory that includes:
- ***Patient's name***
- ***Location in facility***
- ***General condition***

[47] 45 CFR § 164.510(b).

[48] *See* Bulletin #1.

[49] 45 CFR § 164.510(b)(3).

[50] *See* Bulletin #1 and 45 CFR § 164.510(b)(4).

[51] 45 CFR § 164.510(a).

[52] 45 CFR § 164.510(a)(3).

it is consistent with the patient's prior expressed preferences (if known) and in the patient's best interest.[53]

When a facility makes a disclosure for notification purposes or in the facility directory, it is not bound by the accounting requirements.[54] In other words, the facility does not have to record instances in which PHI is disclosed for notification or in the facility directory.

VI. Section 1135 Waiver

Congress has recognized that, in certain situations, enforcement of HIPAA requirements will need to be waived. In 2002, Congress enacted the Public Health Security and Bioterrorism Response Act, which added a Section 1135 to the Social Security Act. Upon a Presidential declaration of emergency or disaster pursuant to the Stafford Act[55] and a Secretarial declaration of public health emergency pursuant to the Public Health Service Act[56], Section 1135 authorizes the

[53] 45 CFR § 164.510(a)(3).

[54] 45 CFR § 164.528(a)(1)(iii).

[55] The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121-5206 (the "Stafford Act"), was created to "provide an orderly and continuing means of assistance by the Federal Government to State and local government in carrying out their responsibilities to alleviate the suffering and damage which result from disasters."(42 U.S.C. § 5121(b)) To accomplish this lofty goal, the Stafford Act establishes a process for requesting and obtaining a Presidential disaster declaration, defines the type and scope of assistance available from the Federal government, and describes the conditions for obtaining that assistance. The Stafford Act requires that "all requests for a declaration by the President that a major disaster exists shall be made by the Governor of the affected State."(42 U.S.C. § 5170) The Governor must make his request through the regional Federal Emergency Management Agency ("FEMA") office and take appropriate action to execute the state's emergency plan. (See *A Guide to the Disaster Declaration Process and Federal Disaster Assistance*, Federal Emergency Management Agency, available at http://www.fema.gov/pdf/rebuild/recover/dec_proc.pdf (last visited December 5, 2006). The Governor's request must include information on the nature and amount of state and local resources that have been or will be committed to alleviating the disaster, an estimate on the amount and severity of damage caused by the disaster, and an estimate of the amount of federal assistance that will be needed. Based on the Governor's request, the President may declare that a major disaster or emergency exists or deny the request.(Id.)

[56] Section 319(a) of the Public Health Service (PHS) Act, authorizes the Secretary of the Department of Health and Human Services (HHS) to declare a public health emergency and "take such action as may be appropriate to respond" to that emergency consistent with existing authorities. (42 U.S.C. § 247d.) The Secretary may declare a public health emergency when, after consultation with public health officials, he finds that "a disease or disorder presents a public health emergency or a public health emergency, including significant outbreaks of infectious diseases or bioterrorist attacks, otherwise exists."(42 U.S.C. § 247d(a))

Secretary of HHS to "temporarily waive or modify the application of" certain Medicare, Medicaid and SCHIP requirements to the extent necessary to exempt healthcare providers from sanctions when emergency circumstances have left them unable to comply with such requirements.[57] Included in the list of requirements for which sanctions can be waived are selected HIPAA requirements.

Specifically, the Secretary can waive sanctions and penalties that arise from noncompliance with the following HIPAA requirements:

- to obtain a patient's agreement to speak with family members or friend;
- to honor a request to opt out of the facility directory;
- to distribute a notice of privacy practices; and
- to provide patients with a right to request privacy restrictions or confidential communications.

While Section 1135 Waivers are generally in effect until the earlier of either the end of the "emergency period" or 60 days from the date the Waiver is first published,[58] waivers of these certain HIPAA requirements are limited to the 72 hour period beginning upon implementation of a hospital disaster protocol.[59] This limitation upon the waiver of these HIPAA requirements applies regardless of the scope or duration of the emergency or "emergency period."[60]

As alluded to above, the Secretary can only issue this Section 1135 Waiver for health care services rendered during an "emergency period" in an "emergency area." The statute defines

[57] 42 U.S.C. § 1320b-5(a)(2).

[58] 42 U.S.C. § 1320b-5(e)(1)(A)-(C). However, pursuant to 42 U.S.C. § 1320b-5(e)(2), the Secretary may provide for an extension of a 60-day period for an additional period or periods. Each extended period can consist of only 60 days.

[59] 42 U.S.C. § 1320b-5(b).

[60] *Id.*

"emergency area" and "emergency period" as the geographical area and period (respectively) in which there is a presidentially declared disaster or emergency under the Stafford Act[61] and a public health emergency as declared by the Secretary under the Public Health Service Act.[62] This means that Section 1135 waivers will not be available for local and state declared emergencies and disasters for which there is no presidential declaration.[63]

Section 1135 Waivers are not available for local and state emergencies.

In the wake of the Presidential declaration of emergency in Louisiana and surrounding states for Hurricane Katrina in August 2005,[64] the Secretary of HHS issued a Section 1135 Waiver related to various statutes and regulations, HIPAA. The Secretary's Section 1135 Waiver exempted hospitals from sanctions for noncompliance only in the four categories listed at the beginning of this section. This means that hospitals were still required to comply with the majority of HIPAA requirements. As mandated by the Social Security Act, this Waiver was only effective for 72 hours after hospitals implemented their hospital disaster protocols.[65] After this 72 hour mark, hospitals had to comply with all HIPAA obligations or risk penalties for noncompliance.

The HIPAA Waiver issued post-Katrina was only effective for 72 hours.

VII. HIPAA Guidance Issued Post Hurricanes Katrina and Rita: Business Associates and Business Associate Agreements

[61] Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121-5206.

[62] Id. and the Public Health Service Act, 42 U.S.C. § 201 et seq.

[63] The EMTALA TAG recently recommended that Section 1135 Waivers be expanded to provide protections to include declared state, county and city emergencies as well as hospital-specific emergencies as determined by CMS/OIG on a case-by-case basis. See note 23.

[64] See Statement on Federal Emergency Assistance for Louisiana issued The White House, August 27, 2005, available at http://www.whitehouse.gov/news/releases/2005/08/20050827-1.html (last visited December 5, 2006).

[65] 42 U.S.C. 1320b-5(b)(3).

A bulletin issued by OCR following Hurricane Katrina provided guidance to covered entities with respect to disclosures to business associates.[66] In general, a health care provider may disclose PHI to a business associate only to the extent permitted in the business associate agreement. There may be instances during an emergency or disaster when needed disclosure of PHI is not within the parameters of the business associate agreement. The provider and business associate may amend the agreement to allow for such disclosure. Where time and circumstances prohibit a formal amendment, however, providers and business associates should proceed with the necessary disclosure and amend the agreement as soon as practicable.

BAAs should be amended to provide for disclosures during a disaster.

Providers should be aware that this specific DHHS waiver of HIPAA liability was posted only in response to Hurricane Katrina, and it cannot be assumed that the same such waiver will apply in future emergency or disaster situations. Health care providers are well-advised to review (and amend, where appropriate) their existing business associate agreements to account for disclosures that may be necessitated by a disaster or emergency.

VIII. Conclusion

There are significant exceptions to HIPAA's stringent Privacy Rule that will allow covered entities to share PHI during emergency and disaster situations, including communicable disease outbreaks. To the extent a hospital's HIPAA policies and procedures do not reflect these exceptions, they should be amended. Hospitals may also consider creating a separate set of HIPAA policies that will only apply during emergency and disaster situations. Regardless of how a

[66] *See* U.S. Department of Health and Human Services Office for Civil Right, "Hurricane Katrina Bulletin #2: HIPAA Privacy Rule Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina," September 9, 2005.

hospital chooses to incorporate the HIPAA exceptions discussed in this paper, employees, staff and providers should be educated on these issues so that their ability to share information is not unnecessarily impeded during a disaster.

Notes