Sharing Protected Health Information with Public Health Agencies, Law Enforcement, and the Media

By Patricia A. Markus
Partner, Nelson Mullins Riley & Scarborough LLP

I. Privacy of Health Information under HIPAA: The General Rule

Generally speaking, the privacy regulations implemented under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Privacy Rule"), as amended by the Health Information Technology for Clinical Health Act, permit "covered entities" (which include, for purposes of this discussion, health care providers, such as hospitals and physicians, and group health plans and health insurers) to use and disclose the protected health information ("PHI") of patients—without obtaining such patients' written consent—only for purposes of **treating** patients, obtaining **payment** for that treatment, and conducting **health care operations** necessary for the ongoing operations of the covered entities.

PHI is defined as any information pertaining to an individual's health care or payment for that care which identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI also may be used and disclosed without patient consent as required or permitted other applicable federal and state laws. When trying to determine whether and under what circumstances a covered entity may disclose an individual's PHI to public health authorities, law enforcement personnel, or the media, covered entities and these potential recipients alike should consider the following additional HIPAA provisions.

It is important to note that each of these listed uses and disclosures is permitted, but not required, by HIPAA. Accordingly, before a covered entity discloses PHI under any of these circumstances, it would be wise to check state and other applicable federal law. If a state or other federal law provides greater protection for PHI or permits patients greater rights of access to their PHI, then the conflicting state or federal law "trumps" HIPAA and is the controlling law.

If HIPAA or other applicable law doesn't permit disclosure of PHI without a patient's written authorization or consent, in many instances such disclosure is permitted if the individual—or the individual's parent, guardian, next of kin, or other personal representative—agrees to the disclosure.

II. Disclosures of PHI Requiring Patient's Opportunity to Agree or Object

The Privacy Rule permits disclosure of PHI without specific patient consent in a few circumstances if the individual is offered an opportunity to agree or object to the disclosure. These circumstances include:

A. Hospital/Facility Directory: Unless the individual objects, a hospital or other health care facility may include information about the individual in its directory, including the individual's name, location in the hospital/facility, the individual's condition in general terms (good, fair, stable, critical), and the individual's religious affiliation.

B. Involvement in Individual's Care: Unless the individual objects, disclosure of the individual's PHI is permitted to a friend or family member or anyone identified by the individual. The PHI disclosed must be directly related to the person's involvement with the individual's health care or payment related to that health care. This includes uses and disclosures of PHI for disaster relief purposes, and if an individual is deceased, disclosure of the individual's PHI to persons involved in the patient's care or payment for care prior to her death is permitted unless the deceased individual previously advised the covered entity not to share PHI with such persons.

III. Disclosures of PHI "Required by Law"

HIPAA permits covered entities to use or disclose PHI if the use or disclosure is required by law, and to the extent the use or disclosure complies with and is limited to the relevant requirements of that law. Examples of uses and disclosures that are required by law include the following:

A. Public Health Activities: covered entities may use and disclose PHI for public health activities to:

1. Public health authorities that are authorized to collect or receive PHI to prevent or control disease, including vital events, or to conduct public health surveillance and investigations;

2. Public health authorities that are authorized to receive reports of child abuse or neglect;

3. A person subject to jurisdiction of the FDA regarding an FDA-regulated product or activity, to (a) collect or report adverse events, product defects or problems, (b) track FDA-regulated products, and (c) enable product recalls;

4. A person possibly exposed to a communicable disease or who may be at risk of contracting/spreading a disease or condition; and

5. A school about a student or prospective student with proof of immunizations, if the school is required by law to have such proof before enrolling the student and the covered entity documents either the parent's (if the student is an unemancipated minor) or the student's agreement to the disclosure

B. Victims of Abuse, Neglect, or Domestic Violence: a covered entity may disclose PHI about an individual whom the covered entity reasonably believes to be a victim of abuse,

neglect, or domestic violence to a government authority authorized by law to receive such reports.

1. Such disclosures must be limited to the information permitted to be disclosed by law and, other than in cases of child abuse or neglect, either must be agreed to by the individual or the must be expressly authorized by law and the covered entity, in the exercise of professional judgment, must believe that the disclosure is necessary to prevent serious harm to the individual or other potential victims.

2. If the individual is unable to agree due to incapacity, the official authorized to receive the report must represent that the PHI is not intended to be used against the individual and that an immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

C. Health Oversight Activities: a covered entity may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for oversight of the health care system or government benefit programs for which health information is necessary for beneficiary eligibility.

D. Judicial and Administrative Proceedings: a covered entity may disclose PHI in response to:

1. A court order; or

2. A subpoena, discovery request, or other lawful process without a court order, if the covered entity receives satisfactory assurance from the party seeking the information that: (a) the person who is the subject of the requested PHI has been given notice of the request; or (b) reasonable efforts have been made by the party seeking the PHI to secure a qualified protective order over the information.

E. Decedents: a covered entity may disclose PHI of a decedent to:

1. A coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; and

2. Funeral directors as needed to carry out their duties with respect to the decedent.

F. Disclosures for Law Enforcement Purposes: HIPAA permits covered entities to disclose PHI to law enforcement authorities under a variety of circumstances, including:

1. Pursuant to legal process (such as a court order, judicial subpoena or summons, grand jury subpoena, administrative subpoena, or civil investigative demand);

2. In response to a request by law enforcement to assist in identifying or locating a suspect, fugitive, material witness, or missing person; the information that may be disclosed is limited to the patient's name, address, date and place of birth, Social Security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death (if applicable), and description of the individual;

3. In response to a law enforcement request for information about victims of a crime, provided the victim agrees to the disclosure or cannot agree due to incapacitation;

4. PHI about a decedent if the purpose of the report is to alert law enforcement of the covered entity's suspicion that the death resulted from criminal conduct;

5. PHI that the covered entity believes is evidence of criminal conduct that occurred on its premises; and

6. PHI of a medical emergency occurring outside the health care provider's premises if the disclosure appears necessary to alert law enforcement that a crime has been committed and the nature and location of the crime, along with the identity, description, and location of the perpetrator.

Note the permissive nature of the language used, the detailed requirements for and limitations of each disclosure, and the fact that the purpose of each of these disclosures is to assist law enforcement in solving, not preventing, a crime.

G. Disclosures to Avert a Serious Threat to Health or Safety: HIPAA permits disclosures of PHI where such disclosures are necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Such disclosures must:

1. Be consistent with other applicable law and standards of ethical conduct; and

2. Be made to a person or persons who are reasonably able to prevent or lessen the threat—including the target of the threat; or

3. Be necessary for authorities to identify or apprehend an individual either:

a. Due to the individual's statement admitting participation in a violent crime that may have caused serious physical injury; or

b. Where it appears a person has escaped from a correctional institution or lawful custody.

Persons "reasonably able to prevent or lessen the threat" can include family members or other individuals, other health care providers, and law enforcement.

Use of the phrase "serious and imminent threat" significantly limits the circumstances under which such disclosures will be permitted under HIPAA.

III. Office for Civil Rights Letter to Health Care Providers

On January 15, 2013, then-Director of the Office for Civil Rights ("OCR"), Leon Rodriguez, sent a letter to the nation's health care providers clarifying the effect of the HIPAA Privacy Rule on threats of violence. The letter informs providers that HIPAA does not prevent their ability to disclose necessary information about a patient to law enforcement, family members of the patient, or others when a patient is believed to present a serious danger to himself or other people who may reasonably be able to prevent or lessen the risk of harm. The letter notes that when a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, the Privacy Rule allows the provider, consistent with applicable law and standards of ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat.

Noting that most states have laws or case law that permit or require disclosure of patient information to prevent or lessen the risk of harm, the letter concludes that providers

> should consult the laws applicable to their profession in the states where they practice, as well as 42 CFR Part 2 . . . to understand their duties and authority in situations where they have information indicating a threat to public safety.

Although the one-and-a-half page letter emphasizes that HIPAA does not prevent health care providers from disclosing information about patients when they are concerned that a patient poses a threat, the letter makes clear that providers must know whether state law and 42 C.F.R. Part 2 (which applies to records of individuals who have been treated or sought treatment at a federally-assisted substance use disorder treatment center) permit their release of mental health or substance use disorder information to third parties under these circumstances.

IV. OCR HIPAA Guidance on Sharing Mental Health Information with Family Members

Under certain circumstances, the HIPAA Privacy Rule permits covered entities to use and disclose PHI if it first provides an individual the opportunity to object. One of these circumstances permits a covered entity to disclose PHI about an individual to a friend, family member, or close personal friend where the PHI disclosed is directly relevant to the person's involvement in the individual's care or payment for that care. If the individual is not present to object due to an emergency or is incapacitated, a covered entity may exercise professional

judgment to determine whether disclosure of directly relevant information to a family member or friend would be in the best interests of the individual.

On February 20, 2014, OCR released revised HIPAA guidance clarifying that:

1. Health care providers are permitted to inform family members of a mental health patient "who has capacity and indicates that he or she does not want the disclosure made," if the patient constitutes a "serious and imminent" threat to the health or safety of self or others, and if the family members notified are in a position to diminish or eliminate the threat.

2. Even in the case where danger is not imminent, the guidance notes that HIPAA allows providers to communicate with patients' family members or other involved in such patients' care about medications, or "about warning signs that may signal a developing emergency," if the patient is given the opportunity to, but does not, object to such disclosures.

3. Providers also may communicate with family members "to be on watch or ensure compliance with medication regimens, as long as the patient has been provided an opportunity to agree or object" to the disclosure and the patient has not objected.

4. HIPAA "in no way prevents" providers from listening to family members or other caregivers who have concerns about a patient's health or well-being, and a provider may "factor that information into" the patient's care—and, presumably, include this information in a determination whether the patient poses a serious and imminent risk to herself or others.

Resources:

https://www.hhs.gov/hipaa/for-individuals/index.html

https://www.hhs.gov/hipaa/for-professionals/index.html

American Health Lawyers Association webinar on "The Intersection of Public Health and Health Care: Health Care Data and the Law in the 21st Century, Sharing Data: Modern Legal Issues and Trends."

- Wednesday, August 9, 1-2:30 pm. FREE to register: https://distancelearning.healthlawyers.org/products/the-intersection-of-public-health-and-health-care-health-care-data-and-the-law-in-the-21st-century-part-iii-sharing-data-modern-legal-issues-and-trends