Research Department

Patrick J. McCormack, Director

600 State Office Building
St. Paul, Minnesota 55155-1298
651-296-6753 [FAX 651-296-9887]
www.house.mn/hrd/

Minnesota House of Representatives

June 15, 2018

TO: Members of the Legislative Commission on Data Practices

FROM: Nathan Hopkins, Legislative Analyst 651-296-5056

RE: Follow-up on questions from June 13 Commission Meeting

This memorandum follows-up on questions that members asked at the June 13 meeting of the Legislative Commission on Data Practices. The following topics are covered:

1. Disclosure of protected health information ("PHI") for research purposes under HIPAA and the MHRA.
2. What happens to money collected by the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) when it imposes civil monetary penalties?
3. Under HIPAA, what is the status of patient directory information?
4. Under HIPAA, what is the distinction between internal fundraising and marketing?
5. Under HIPAA, what kind of criminal penalties can be imposed against a corporation?

1. Disclosure for research purposes: HIPAA vs MHRA

- **HIPAA**
  - Research is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." See 45 CFR § 164.501.
  - *Unless the researcher is also a covered entity under HIPAA (e.g. the researcher is providing health care as part of a clinical trial for a drug), the researcher is not subject to HIPAA, including its privacy rule, its security rule, and its breach notification rules. Only the covered entity that discloses data to the researcher is subject to HIPAA.*
    - Although a researcher is not necessarily subject to HIPAA, there are federal regulations requiring human-subject researchers to protect individual privacy and confidentiality. Per HHS and FDA Regulations (45 CFR § 46.111(a)(7) and 21 CFR § 56.111(a)(7)), an Institutional Review Board (IRB) shall determine that where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain confidentiality of data in order to approve human subjects research.

- A covered entity may always use or disclose for research purposes health information which has been de-identified (in accordance with 45 CFR §§ 164.502(d), and 164.514(a)-(c) of the rule).
- Under the privacy rule, PHI may be disclosed for research purposes only with individual authorization, or without individual authorization under these limited circumstances:
  - With documented approval from an IRB or privacy board
    - An IRB is a board, committee, or other group formally designated by an institution to review research involving humans as subjects. IRBs have authority to approve, require modification to, or disapprove all research activities covered by the HHS and FDA Protection of Human Subjects Regulations. More importantly here, IRBs also have authority to approve a waiver or an alteration of the privacy rule's authorization requirement for research purposes. Similarly, a privacy board is a review body that is established specifically to act upon requests for a waiver or an alteration of the authorization requirement under the privacy rule for uses and disclosures of PHI for a particular research study.
    - A covered entity may use or disclose PHI for research purposes without patient authorization if an IRB or privacy board waives the individual authorization requirement. To waive the individual authorization requirement for research, the IRB or privacy board must find that: (1) the use or disclosure of PHI involves no more than a minimal risk to individual privacy, based on specific criteria; (2) the research could not practically be conducted without the waiver; and (3) the research could not practically be conducted without access to and use of PHI. *See* 45 CFR § 164.512(i).
  - As a limited data set with a data use agreement
    - This requires a data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher for research, public health, or health care operations. *See* 45 CFR § 164.514(e). A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual.
  - For preparation in advance of research
    - This requires representations from the researcher, either in writing or orally, that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any PHI from the covered entity, and representation that PHI for which access is sought is necessary for the research purpose. *See* 45 CFR § 164.512(i)(1)(ii). This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.

- For research on decedents' information
  - This requires representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. *See* 45 CFR § 164.512(i)(1)(iii).

- In general, the privacy rule gives individuals the right to receive an accounting of certain disclosures of PHI made by a covered entity. *See* 45 CFR § 164.528.
  - This accounting must include disclosures of PHI that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose. *See* 45 CFR § 164.528(b)(3).

- **MHRA**
  - Health records may be released without a patient's consent, so long as the patient does not object. *See* Minn. Stat. § 144.295.
    - To release health records (generated in 1997 or after[1]) to an external researcher, a provider must:
      - disclose to current patients that health records may be released unless the patient objects; *and*
      - use "reasonable efforts" to obtain a patient's written authorization to release health records.
        - it is sufficient for a provider
        - this authorization does not expire, but may be revoked or limited by the patient at any time
    - If a provider twice attempts to notify a patient by mail that their medical records may be released to an external researcher, and no objection is received, patient authorization is established.
  - At a patient's request, a provider must provide the patient with information about how to contact an external researcher to which the patient's records were released.
  - When a provider releases health records to an external researcher, the provider must make a "reasonable effort to determine" that:
    - the use or disclosure does not violate limitations under which the record was collected;
    - individually identifiable information is necessary for the research;

[1] Health records generated before January 1, 1997, may be released unless the patient has objected. *See* Minn. Stat. § 144.295.

- the researcher has adequate safeguards in place to protect the security of the records; and
- that further release of the records in individually identifiable form is prohibited.

- A provider who discloses records to a researcher without patient consent must document what records were released, to whom, and when. *See* Minn. Stat. § 144.293, subd. 9.

2. What happens to money collected by OCR for civil monetary penalties?

- Under the HITECH act of 2009, money collected by the OCR is transferred to OCR "to be used for purposes of enforcing the provisions" of HIPAA. *See* 42 USC § 17939(c)(1).
- This section of the law also requires HHS to establish regulations to distribute a percentage of collected penalty money to harmed individuals. This should have been completed by 2012. *See* 42 USC § 17939(c)(3). Nevertheless, as of the 2013 publication of the final rule for implementing the HITECH act, no such regulations have been enacted. *See* 75 FR 40868-01 ("we do not address in this rulemaking . . . the penalty distribution methodology requirement in section 13410(c) of the Act, which is to be based on the recommendations noted above to be developed at a later date by the GAO").

3. Under HIPAA, what is the status of directory information?

- It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information.
- Unless an individual objects, a covered health care provider may rely on an individual's *informal permission* to list in its facility directory the following PHI:
  - individual's name,
  - general condition,
  - religious affiliation, and
  - location in the provider's facility.
- This information may be disclosed *only* to members of the clergy or (excepting religious affiliation) to other persons who ask for the individual by name. *See* 45 CFR § 164.510(a). The information nevertheless remains PHI and cannot be further disclosed or sold to other parties.

4. Under HIPAA, what is the difference between internal fundraising and marketing?

Different rules apply for the use of PHI for marketing and for fundraising. A covered entity cannot use a patient's PHI for marketing purposes without patient authorization. A covered entity may use a patient's PHI for fundraising without patient authorization. A discussion of each follows.

- **Marketing**: A covered entity must obtain a patient's authorization for any use or disclosure of PHI for marketing, unless the communication is a face-to-face communication between a provider and the patient or the communication is a promotional gift of nominal value. *See* 45 CFR § 164.508(a)(3).
    - "Marketing" is defined as a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service. These are not marketing:
        - refill reminders or other communications about a drug or biologic currently prescribed for the patient
        - a communication for a provider to treat a patient, including case management or care coordination, or to direct or recommend alternative treatment
        - describing a health-related product or service that is provided by or covered by the covered entity making the communication
        - other case management and care coordination communications, to the extent these are not considered treatment
- **Fundraising**: A covered entity may use a specific set of information for purposes of fundraising for its own benefit, *without* obtaining patient authorization. *See* 45 CFR § 164.514(f).
    - The information that may be used without patient authorization is demographic information relating to the patient (name, address, other contact information, age, gender, and date of birth); dates of health care provided to the patient; treating physician, outcome information, health insurance status, and information on department of service.
    - A covered entity can also share this information for fundraising purposes with a business associate or to an institutionally related foundation.
    - With each fundraising communication, a covered entity must include a notice that the patient can opt out of further fundraising communications. If a patient opts out of fundraising communications, the covered entity is prohibited from sending them.
    - A covered entity cannot require a patient to receive fundraising communications, as a condition of providing treatment.

5. Under HIPAA, what kind of criminal penalties can be imposed against a corporation?

- To knowingly[2] obtain or disclose PHI in violation of HIPAA is a federal offense, and the U.S. Department of Justice ("DOJ") may prosecute individuals or corporations for a violation. *See* 42 USC § 1320d-6.

[2] "Knowingly" does not mean that a person has to know that they are breaking the law. It requires only proof of knowledge of the facts that constitute the offense.

- Applicable criminal penalties under HIPAA are as follows:
    - A fine of up to $50,000 and/or imprisonment for up to one year
    - If the offense is committed under false pretenses, a fine of up to $100,000 and/or imprisonment for up to five years
    - If the offense is committed with intent to use PHI for personal gain or malicious harm, a fine of up to $250,000 and/or imprisonment for not more than ten years
- While a corporation cannot be imprisoned, it may be subject to criminal fines. A court may also order a corporation to remedy any harm caused by the offense. A court can also place a corporation on probation. Probation is intended to ensure that a convicted corporation complies with obligations to pay fines or make restitution, but can come with a variety of court-ordered conditions. *See generally* U.S.S.G. § 8D.1.
- In a clarifying memorandum regarding these prosecutions, DOJ's Office of Legal Counsel ("OLC") has stated that *only covered entities (and their employees) may be by criminally prosecuted for HIPAA violations*.
    - Nevertheless, individuals not directly subject to HIPAA may be criminally liable indirectly under principles of "aiding and abetting" and conspiracy liability.
- In general, crimes committed by a corporation's employee may be imputed to the corporation when the employee is acting within the scope of his employment. The criminal intent of an employee (i.e. the "knowingly" element of the crime) may also be imputed to the corporation when the employee acts on the corporation's behalf.
- Conversely, it is possible for the criminal liability of a corporation to be attributed to individuals in managerial roles, though this is extremely rare. The OLC memo mentioned above also states that "certain directors, officers and employees of [covered] entities may be liable directly . . . in accordance with general principles of corporate criminal liability.

NH/jg