

## **Don't Ask, Don't Tell? Transfer and Sale of De-Identified Patient Data**

**By Gabrielle B. Goldstein and Jill H. Gordon**

### **Introduction**

Advances in bioinformatics and automated laboratory equipment have made it possible to "mine" very large medical databases and repositories of biological samples for information that will ultimately produce novel therapies. Some physicians and hospitals have noted the commercial implications of this research and have begun to charge pharmaceutical companies and biomedical researchers fees for medical data and biological specimens obtained during patient care. Commercialization of this emerging area of research has made it more important to address issues that relate to the original source of the information and samples: patients and clinical research subjects (in this article, collectively referred to as "patients"). Three major issues are informed consent, confidentiality and conflicts of interest:

- Must healthcare providers obtain consent from individuals before selling or transferring their medical data and samples?
- What safeguards govern the confidentiality afforded to such data and samples?
- Must healthcare providers disclose the compensation they receive from such sale or transfer to the individuals involved? Further, must such disclosure be made even in the absence of a law that specifically requires the healthcare provider to obtain patient authorization for the sale or transfer of such medical data?

The HIPAA Privacy Rule, state laws, and case law provide potential answers and guiding principles for answering these questions.

### **HIPAA Privacy Rule**

#### **Applicability**

Currently, there are no federal or state laws governing ownership of an individual's medical data or biological materials. However, there are both federal and state laws that govern the right to privacy, particularly of medical information. The federal HIPAA Privacy Rule regulates the use and disclosure of individually identifiable health information (also known as protected health information or PHI) held by certain individuals and organizations defined by statute as "covered entities".<sup>1</sup> PHI is defined as health information that either identifies an individual or with respect to which there is a reasonable basis to believe the information could be used to identify an individual.<sup>2</sup> Covered entities include healthcare plans, clearinghouses that handle payments, and healthcare providers who electronically transmit PHI in connection with activities such as billing, payment, and reimbursement.<sup>3</sup> Hospitals and physicians are HIPAA covered entities, because such entities fit within the definition of "healthcare provider," which specifies that the person, business or agency "furnish, bill or receive payment for healthcare in the normal course of business."<sup>4</sup>

#### **Privacy Rule and Research**

The Privacy Rule provides assurance that one's PHI will not be used or transferred without authorization. In the research context, the Privacy Rule is implicated in two central instances. First, when a covered entity wishes to disclose PHI to a researcher upon the researcher's request, and second when a covered entity is itself engaged in research, and wishes to use PHI already in the entity's possession to conduct research.<sup>5</sup> Patient

authorization is required in both instances because the Privacy Rule specifically states that a covered entity may not “use or disclose” PHI without authorization.<sup>6</sup> Thus, for instance, a physician may not use PHI for his/her own research purposes simply because he/she has already obtained the data for clinical purposes.

Although the Privacy Rule provides assurance that PHI cannot be used or disclosed without authorization, it does contain exceptions. In particular, the Privacy Rule excepts the following uses and disclosures of PHI without prior patient authorization for research purposes:

1. If the covered entity only uses or discloses a limited dataset pursuant to a data use agreement between the healthcare provider and a researcher or research institution
2. If review of the PHI is necessary to prepare a research protocol or is otherwise preparatory to research
3. If a privacy board or IRB acting as a privacy board has waived the authorization requirement for subject recruiting purposes
4. If the research involves data on decedents<sup>7</sup>

### **De-Identified Information**

The Privacy Rule protects PHI, but not data and samples that are excluded by the definition of PHI. Therefore, covered entities need only obtain authorizations for use or disclosure of personally identifiable health information. Covered entities are always able to use and disclose patient information that does not rise to the level of constituting PHI.<sup>8</sup> Once patient information is de-identified in accordance with one of the Privacy Rule’s two methods of de-identification, a covered entity may use and disclose the de-identified information free of patient authorization or other restrictions. Permitted use and disclosure includes the sale or transfer of patient data and samples to databases, repositories, researchers and even pharmaceutical companies.

The Privacy Rule provides two methods by which covered entities can de-identify PHI. The first method requires that a person with “appropriate knowledge of and experience with” relevant statistical analyses determine and document the determination that the risk is very small that the information could be used to identify an individual.<sup>9</sup> The second requires that a covered entity remove 18 identifiers from the information, and the covered entity has no actual knowledge that the remaining information could be used to identify an individual.<sup>10</sup> The list of 18 identifiers is quite broad, including items such as birth date and county of residence. The last item in the list is “any other unique identifying number, characteristic, or code.”<sup>11</sup> Many research institutions take the position that biological material can be “deidentified” in accordance with the Privacy Rule, but it is currently an open question as to whether this last item precludes the unauthorized use or transfer of biological samples, all of which include DNA and RNA, molecules that are unique to each individual.

Thus, leaving aside the DNA/RNA question, if a healthcare provider such as a hospital or physician de-identifies patient data in accordance with one of the Privacy Rule’s de-identification methods described above, that healthcare provider is free to use, disclose or transfer the de-identified data and samples, for free or for charge, and will not be subject to any HIPAA restrictions regarding such activities.

### **State Law**

HIPAA provides a baseline of coverage and protection for protected health information; however, state law can provide more protection than HIPAA. In such case, HIPAA does not preempt the more protective elements of state law.<sup>12</sup>

State law protections are generally only afforded to personally identifiable health information. For example, the Confidentiality of Medical Information Act (CMIA), housed in

the California Civil Code, regulates the use and disclosure of medical information in California. CMIA is the state law analog to HIPAA, but HIPAA will preempt any discrepancies should CMIA prove less stringent or otherwise conflict with HIPAA. CMIA arguably contains provisions more stringent than HIPAA regarding use and disclosure of individually identifiable patient information. For example, it applies to paper-based as well as electronic records. However, because CMIA defines "medical information" as "individually identifiable data," the statute does not govern the sale or use of de-identified health data.<sup>13</sup> Some states, including Illinois, have statutes that preclude the disclosure of medical information (including de-identified information) during litigation except in circumstances that are narrower than the circumstances available under HIPAA. However, such statutes are confined to the context of evidence discoverable during litigation, and are thus outside of the scope of this article.

### **Property Rights and Conflict of Interest**

If a healthcare provider is fully compliant with federal and state laws governing patient privacy, does it still have an additional obligation to disclose to the patients any financial relationships with recipients of the data and samples? Do you have a right to know if your physician plans to sell your data and biological samples to a company that may use them to create a highly profitable new medical product? These questions apply even if the data has been de-identified. The prospect of earning revenue from such sales may affect your healthcare provider's decisions, such as whether to enroll you in a clinical trial. Your physician may order unnecessary tests (at your expense) that yield profitable data and samples. Your physician may sincerely believe that the extra tests are medically justified, but his/her judgment may be unconsciously clouded by the financial aspects. Certainly, Medicare has excluded many thousands of physicians for performing or ordering unnecessary medical services for financial reasons. In the absence of requirements to disclose such conflicts of interest, is the trusting relationship between physician and patient diminished because the patient cannot know for sure about such financial conflicts of interest?

In the context of medical care, the issues of informed consent and disclosure of conflicts of interest are largely a creature of state case law rather than statutory law, where it has been addressed at all. For example, the leading California case on conflicts of interest at the crossroads of medicine and research is *Moore v. The Regents of the University of California*, 51 Cal. 3d 120 (Cal. 1990). In *Moore*, the plaintiff sued based on conversion, breach of fiduciary duty, and lack of informed consent after a physician sold part of the plaintiff's spleen for commercial research purposes without the patient's consent. (Black's Law Dictionary defines conversion as the "wrongful possession or disposition of another's property as if it were one's own". Breach of fiduciary duty is a violation of a legal or moral obligation owed to another, such as the duty of a physician to obtain the patient's informed consent prior to treatment.) The California Supreme Court made two central holdings: first, that persons in California do not have a property interest in their biological samples, and thus the conversion claim failed, and second, that persons in California do have a right to determine in an informed manner whether or not to submit to medical treatment, and physicians do have a duty to obtain such informed consent. In other words, if a medical treatment includes taking a biological sample, the patient has the right to informed consent with respect to use of that sample, and the treating physician has the duty to obtain that consent.

Does the *Moore* case apply to the sale and transfer of de-identified data and samples? With respect to property rights and conversion, the facts in *Moore* are distinguishable from a situation in which a physician or other healthcare provider sells or transfers de-identified data. The *Moore* case dealt with the status of biological samples and materials, not patient

data (much less de-identified data). It is a stretch to equate the Moore physician's sale of his patient's spleen tissue with a physician who sells patient de-identified data. But even if such a parallel could be drawn, one of the central holdings in Moore was the proclamation that people in California do not have a property right in their cells or other biological material. It seems logical that if there is no property right in one's biological material, one would not have a property right in one's data, and in particular, data de-identified in a manner deemed acceptable under the HIPAA Privacy Rule. Therefore, according to Moore, patients whose de-identified data or medical samples are sold would likely not have a viable claim for conversion.

However, the California Supreme Court also held in Moore that the physician violated his fiduciary duty to his patient, and his patient should have been had the opportunity to give informed consent about potential tissue sales prior to surgery. The Court reached this conclusion because persons have the right to determine whether or not to submit to medical treatment, and for such consent to be informed, a physician must exercise his/her fiduciary duty to disclose all information that may be material to the patient's decision. Importantly, the Court held that a physician's personal or financial interest in a patient's biological material is information that would be material to a patient's decision, and thus must be disclosed for consent to be informed. Moore has been cited numerous times in the courts of several states and federal jurisdictions for the proposition that a physician's failure to obtain proper informed consent prior to medical treatment can lead to a valid tort action, and that a physician must disclose financial interests in order for consent to treatment to be informed.<sup>14</sup>

If healthcare providers that enter into financial arrangements for the sale or transfer of de-identified patient data wish to avoid liability under Moore and any appearance of conflict, there is a solution: They can place information about the potential sale or transfer of de-identified information and biological samples in their notice of privacy practices. HIPAA requires that physicians who have a direct treatment relationship with patients make a good-faith effort to obtain written acknowledgments from those individuals that they have received the provider's notice.<sup>15</sup> If a physician with financial arrangements for the sale or transfer of de-identified patient data wishes to add information to the notice of privacy practices to avoid the appearance of a conflict and to discharge his or her duty to disclose all material information, the physician could add the following statement:

"We may sell or transfer your de-identified health information and biological samples to third-parties for use in research. Prior to any sale or transfer, all data that might identify you will be removed."

Patients may find this disclosure relevant to their healthcare decisions. Providing such information to patients limits potential exposure to liability under Moore and alleviates the appearance of a conflict of interest.

## **Conclusion**

Under the HIPAA Privacy Rule, healthcare providers such as hospitals and physicians can donate or sell patient data and biological samples to research foundations or commercial repositories without patient authorization, provided such data is de-identified in accordance with HIPAA. However, a separate and independent inquiry involves whether healthcare providers must disclose any financial compensation they may expect from the sale or transfer of data or samples in order to obtain informed consent for the medical care they render. In other words, physicians may do everything right under HIPAA, but they still have a duty to disclose relevant financial interests to their patients. Healthcare providers that enter into financial arrangements with researchers and repositories may wish to consider including a disclosure of the potential use or transfer of de-identified data and samples in

their notices of privacy practice in order to avoid the appearance of a conflict of interest. Also, they should confirm that their proposed transfer of data complies with applicable state law.

## References

1. 45 CFR 160.103.
2. 45 CFR 164.501.
3. 45 CFR 160.103.
4. 45 CFR 160.103.
5. Tovino, The Use and Disclosure of Protected Health Information for Research under the HIPAA Privacy Rule, 49 S.D. L. Rev. 447, 451 (2003/2004).
6. Tovino, Id.
7. 45 CFR 164.512(i).
8. Tovino, 45 S.D. L. Rev. 447, 455.
9. 45 CFR 164.514(b)(1).
10. 45 CFR 164.514(b)(2). The 18 identifiers are as follows: names; geographic subdivisions smaller than a State, including street address, city, county, and full zip code; all elements of dates except year, including birth and admission dates; phone numbers; fax numbers; email addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers; device identifiers; URLs; IP addresses; biometric identifiers including finger and voice prints; full face photos and comparable images; other unique identifying numbers, characteristics or codes.
11. 45 CFR 164.514(b)(2)(i)(R).
12. Betzel, 2005-2006 Privacy Year In Review: Privacy Law Developments in California, 2 ISJLP 831 (Fall 2006).
13. Cal. Civil Code § 56 et seq.
14. See DeGennaro v. Tandon, 873 A.2d 191, 199 (Conn. App. Ct. 2005). Court held that if provider-specific information would be material to a reasonable patient in deciding whether to embark on a course of therapy, including potential financial gains, a provider has a duty to disclose that information to the patient in order to obtain that patient's informed consent. See also Heinrich ex rel. Heinrich v. Sweet, 308 F.3d 48, 51 (1<sup>st</sup> Cir. Aug. 22, 2002). The law regarding whether medical researchers who are not providing healthcare to individuals owe a duty to those individuals to obtain informed consent is unsettled, and is beyond the scope of this article. See Greenberg v. Miami Children's Hosp. Research Inst., Inc., 264 F. Supp. 2d 1064 (2003).
15. 45 CFR 164.520(c)(2).

## Authors

Gabrielle B. Goldstein is a healthcare and life sciences attorney in the San Francisco office of Davis Wright Tremaine LLP. She provides hospitals, healthcare providers, and biotechnology companies with regulatory and business advice. She has particular expertise in human subjects research and clinical trial compliance, and advises hospitals and technology companies on IRB, clinical trial, CRO and FDA issues. Contact her at 1.415.276.6573 or GabrielleGoldstein@dwt.com.

Jill H. Gordon is a healthcare and life sciences attorney in the Los Angeles office of Davis Wright Tremaine LLP. She represents hospitals, medical groups and other healthcare entities with regulatory and transactional matters. She advises clients regularly on fraud and abuse issues and on physician self-referral laws. Her expertise includes negotiations on behalf of providers for agreements such as payor contracts, leases, medical director

agreements, and physician recruitment arrangements.. Contact her at 1.13.633.6875 or [jillgordon@dwt.com](mailto:jillgordon@dwt.com).