Crimes and Sanctions: Current Controversies over HIPAA's Criminal Penalty

by Robert Gellman

In the past year there have been some surprising twists in the interpretation of HIPAA's criminal penalty. This article reviews current views of the penalty and considers the effect on sanctions for healthcare workers who fail to comply with health privacy policies.

The Statute and the Rule: What's the Difference?

Most people who talk about HIPAA are referring to the privacy rule promulgated by the secretary of the Department of Health and Human Services.[1] The HIPAA statute authorized the secretary to issue the HIPAA privacy rule. The distinction between the statute and the rule is important to this discussion.

The statute defines the punishment for a criminal violation but fails to define what specific conduct is wrongful. The HIPAA privacy rule contains the standards (e.g., access, authorization, disclosure, minimum necessary) that determine what is improper conduct.

The criminal penalty applies to a person who knowingly and in violation of the HIPAA privacy rule obtains or discloses patient health information. Punishment can include a $250,000 fine and 10 years in prison for trafficking in information for commercial advantage, personal gain, or malicious harm.[2]

The HIPAA privacy rule applies to covered entities, which include most healthcare providers, all health plans, and all healthcare clearinghouses. The question then remains whether the criminal penalty applies only to covered entities or whether it can apply to any person who violates the statute.

A Legal Question

The Office of Legal Counsel (OLC) at the Department of Justice often provides opinions on legal questions that affect the government. On June 1, 2005, OLC concluded that the HIPAA criminal penalty applies only to covered entities.[3]

The opinion removed many healthcare workers from the possibility of criminal liability under HIPAA. A physician at a hospital is a covered entity and may be criminally liable for wrongful conduct. However, a ward clerk is not a covered entity because the clerk is not a healthcare provider who bills for services. Many employees of covered entities are not covered entities for the same reason. A business associate is not usually a covered entity either. A covered entity's employees and business associates remain subject to HIPAA rule. Only application of the criminal penalty is in question.

The OLC opinion removes the possibility of criminal liability under HIPAA from a hacker who steals health records from a hospital computer. If an individual bribes a hospital orderly to provide a copy of a patient record, neither party could be prosecuted under HIPAA.

The OLC opinion is controversial for legal, policy, and other reasons. The line drawn by OLC is so narrow that inappropriate conduct would not be subject to the HIPAA criminal penalty. Consider the case of the healthcare worker who stole patient information for identity theft and was the first individual prosecuted and convicted under HIPAA. That individual could not have been prosecuted under HIPAA had the opinion been issued earlier. Some see political motivations behind the opinion.[4] Regardless, the OLC opinion is binding on federal agencies, although the courts could reach a different conclusion.

Other Criminal Statutes

Whatever the merits of the OLC interpretation, other criminal statutes may be applicable to the conduct not subject to the HIPAA criminal penalty. An article published by Peter Winn, an assistant US attorney active on legal healthcare issues, points the way to an alternative theory.[5] While Winn does not speak for the Justice Department on HIPAA criminal matters, his article on the subject of criminal prosecutions under HIPAA was reprinted in a department publication. That suggests, at a minimum, that the department does not disagree with his conclusions.

Winn points to 18 USC § 2, which establishes a criminal penalty covering any person who willfully causes an act which, if performed by another, would be a criminal offense. In other words, if a person is not capable of committing a violation under a criminal statute, that person can nevertheless be criminally liable for an act that would have been a crime if committed by the person's principal. So in a HIPAA case, a hospital worker who is not a covered entity and who sells a patient record could be criminally liable under 18 USC § 2 because the sale would violate HIPAA if done by the covered entity that employed the worker.

The criminal sanction that the OLC opinion appeared to have eliminated for many employees and business associates of HIPAA covered entities comes back to life as a real criminal penalty courtesy of 18 USC § 2. To prove the point, subsequent to the OLC opinion, the Justice Department successfully prosecuted an employee at a doctor's office who sought to sell health records for personal gain.[6]

Despite all the legal controversies—both past and continuing—we end up mostly where we began. Most conduct that any healthcare worker or patient would inherently recognize as patently offensive remains subject to criminal sanction. Criminal penalties still appear available to be imposed against covered entities and against employees and business associates of covered entities who wrongfully disclose patient information for commercial advantage, personal gain, or malicious harm.

Questions remain about the ability of the HIPAA criminal penalty to reach wholly independent parties (e.g., a purchaser of a record or a hacker), but criminal provisions unrelated to HIPAA may be available. Other nuances of the HIPAA criminal penalty and of criminal law in general remain beyond the scope of this general analysis.

A Word about Sanctions

Does this legal issue affect HIPAA's employer sanction requirement? The privacy rule defines a series of administrative requirements for covered entities. One of those requirements is for the maintenance and application of appropriate sanctions against members of the work force who fail to comply with the privacy policies and procedures of the covered entity or the requirements of the HIPAA privacy rule.[7]

Administrative sanctions are not premised on the availability of criminal penalties. A covered entity's sanctions can be for violation of the entity's privacy policies and procedures. Failing to comply with the requirements of the HIPAA privacy rule is an independent basis for imposing sanctions.

Consider a hospital worker who makes a disclosure permitted under the hospital's policy and under HIPAA. Assume that the worker failed to obtain supervisor approval for the disclosure as required by the hospital's policy. Supervisor approval is a local workplace rule and not a HIPAA privacy rule requirement. The failure to follow the hospital's workplace rule is not subject to criminal sanction under HIPAA under any theory. Nevertheless, the worker could be appropriately sanctioned under HIPAA despite the lack of availability of criminal sanctions.

In countless speeches about HIPAA, lawyers have scared healthcare workers and institutions about the possibility of going to prison for 10 years. Fears about criminal penalties have been vastly overblown. In the more than three years since the HIPAA privacy rule took effect only two criminal cases have been brought.

Both cases involved overt trafficking in patient information. No covered entity or healthcare worker has been prosecuted for any other violation of HIPAA. The likelihood that a routine negligent or inadvertent act would lead to criminal prosecution appears to be extraordinarily small indeed.

In the end, the recent flap about the HIPAA criminal penalty appears to be mostly a fight among lawyers. For the most part, some criminal penalty remains available to address conduct by healthcare workers that everyone would acknowledge to be improper. Administrative sanctions also continue to be available for failures to safeguard privacy or comply with the HIPAA rule.

Despite all the lawyering, the obligations of healthcare workers to protect health information remain firmly in place. Failure to comply with those obligations can result in a variety of criminal or administrative sanctions.

Notes

1. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. 45 CFR Parts 160, 164. August 21, 1996. Available at http://aspe.hhs.gov/admnsimp.
2. Ibid, 42 USC § 1320d-6.
3. "Scope of Criminal Enforcement under 42 U.S.C. § 1320d-6." June 1, 2005. Available online at www.usdoj.gov/olc/hipaa_final.htm.
4. Swire, Peter. "Justice Department Opinion Undermines Protection of Medical Privacy." Center for American Progress. June 7, 2005. Available online at www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=743281.
5. Winn, Peter. "Criminal Prosecutions under HIPAA." United States Attorneys' Bulletin 53, no. 5 (2005). Available online at www.usdoj.gov/usao/eousa/foia_reading_room/usab5305.pdf.
6. United States Attorney's Office, Southern District of Texas. "Alamo Woman Convicted of Selling FBI Agent's Medical Records." Press release. March 7, 2006. Available online at www.usdoj.gov/usao/txs/releases/March2006/060307-Ramirez.htm.
7. HIPAA, 45 CFR § 164.530(e)(1).

***Robert Gellman** (bob@bobgellman.com) is a privacy and information policy consultant in Washington, DC.*

Article citation:
Gellman, Robert. "Crimes and Sanctions: Current Controversies over HIPAA's Criminal Penalty." *Journal of AHIMA* 77, no.9 (October 2006): 96-97,106.