OCR Relies on Corrective Action, Not Civil and Criminal Sanctions, During First Year of Privacy Rule Enforcement

Stacey A. Tovino
satovino@central.uh.edu
October 15, 2004

Last month, the United States General Accountability Office (GAO) issued a report entitled, “Health Information: First-Year Experiences Under the Federal Privacy Rule” (Report).¹ Although the Report does not provide any information from the federal Department of Health and Human Services (HHS) or the Office for Civil Rights (OCR) further interpreting the privacy rule, as many had hoped, the Report does identify and discuss: (1) the experiences of health care providers, health plans, public health entities, researchers, and patients relating to implementation of the privacy rule;² (2) the GAO’s recommended changes to the rule;³ and (3) data and statistics relating to the OCR’s enforcement of the rule.⁴ The Report is valuable for demonstrating that OCR has relied on corrective action, and not civil or criminal sanctions, during its first year of enforcing the privacy rule.⁵

On December 28, 2000, HHS issued a final privacy rule⁶ designed to implement one portion of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).⁷ The privacy rule generally requires covered entities (defined to include all health plans, all health care

² Id. at 1.
³ Id. at 24.
⁴ Id. at 22.
⁵ Id. at 22.
clearinghouses, and many health care providers) to adhere to certain information use and disclosure requirements, patients’ rights requirements, and administrative requirements. The deadline by which most covered entities were required to comply with the rule was April 14, 2003. In its September Report, the GAO found that covered entities’ implementation of the privacy rule during the first year following the compliance deadline “went more smoothly” than expected, that “initial confusion has diminished,” and that “new privacy procedures have become routine practice for their members’ staff.” The GAO also found, however, that covered entities continue to struggle to interpret many provisions within the Privacy Rule including the accounting of disclosures requirement and the business associate provisions.

The accounting of disclosures requirement generally requires covered entities to provide patients with an accounting, or list, of instances in which the entity has disclosed the patient’s protected health information if the patient requests an accounting. The regulation is particularly tricky to apply because it identifies numerous disclosures that covered entities are not required to include in an accounting. According to the GAO Report, covered entities spend significant time and resources attempting to identify and track those disclosures for which an accounting may be requested. For example, the

---

8 45 C.F.R. §§ 164.502-.514.
9 Id. §§ 164.520-.528.
10 Id. § 164.530.
11 Id. § 164.534.
12 GAO REPORT, supra note 1, at 2.
13 45 C.F.R. § 164.528.
14 Id. § 164.528(a)(1)(i)-(ix). The excepted disclosures are those necessary: (1) to carry out treatment, payment and health care operations; (2) to individuals of protected health information about them; (3) incident to a use or disclosure otherwise permitted or required by the privacy rule; (4) pursuant to an authorization; (5) for the facility’s directory or to persons involved in the individual’s care or other notification purposes; (6) for national security or intelligence purposes; (7) to correctional institutions or law enforcement officials; (8) as part of a limited data set; and (9) that occurred prior to the compliance date for the covered entity.
15 GAO REPORT, supra note 1, at 10.
Report indicates that many covered health plans will keep information relating to one enrollee in separate electronic or paper systems relating to enrollment, claims payment, and customer service, which makes it difficult to track each time one of the plan’s systems has disclosed the enrollee’s information.\textsuperscript{16} By further example, the Minnesota Department of Public Health has identified over fifty state statutes that permit or require Minnesota covered entities to disclose information to state or local organizations. Because these disclosures must be included in an accounting, Minnesota covered entities have expressed significant concern about the volume of disclosures they must track.\textsuperscript{17} Finally, many organizations interviewed by the GAO questioned whether the accounting requirement generates much benefit for patients because covered entities have received few or no requests from patients or enrollees for accountings since the April 14, 2003, compliance date.\textsuperscript{18} The GAO ultimately recommended that HHS modify the privacy rule to exempt disclosures to public health authorities from the accounting requirement and to require covered entities to inform patients through their notices of privacy practices that patient information will be disclosed to public health authorities.\textsuperscript{19} HHS responded to a draft of the GAO Report by explaining that it had considered such a change in the past and “continues to monitor the need to modify the Privacy Rule.”\textsuperscript{20}

The Report further indicates that many covered entities have struggled to interpret and apply the business associate provisions set forth in the privacy rule. Under the rule, a covered entity may disclose protected health information to a business associate (including, but certainly not limited to, certain law firms, accounting firms, billing and

\textsuperscript{16} Id. at 11.
\textsuperscript{17} Id.
\textsuperscript{18} Id.
\textsuperscript{19} Id. at 24.
\textsuperscript{20} Id. at 25.
collections companies, and computer software companies) if the covered entity obtains satisfactory assurances, in the form of a business associate agreement, that the business associate will appropriately safeguard the information received from the covered entity.\textsuperscript{21}

The Report indicates that many large covered entities have spent significant resources developing, negotiating, customizing, and executing thousands of business associate agreements because business associates regard the agreements as an opportunity to attempt to include new provisions unrelated to patient privacy.\textsuperscript{22}

The GAO report further indicates that: (1) important biomedical and behavioral research may be delayed due to the varying ways in which covered entities interpret and respond to the privacy rule’s research provisions;\textsuperscript{23} (2) patients face obstacles when seeking access to their protected health information, as generally permitted by the privacy rule;\textsuperscript{24} (3) patients are not aware of their other rights under the privacy rule (such as the right to request additional privacy protection, to request amendment of incorrect protected health information, and to request an accounting of disclosures);\textsuperscript{25} and (4) many patients misunderstand key elements of the privacy rule.\textsuperscript{26}

The enforcement data and statistics contained in the GAO’s Report show that as of May 2004 the OCR had not recommended a single criminal or civil sanction against any covered entity for privacy violations (although the United States Attorney’s Office for the Western District of Washington did file a one-count charge against defendant Richard W. Gibson for knowing and intentional patient identity theft on August 18,

\textsuperscript{21} 45 C.F.R. § 164.502(e)(1)(i); 45 C.F.R. § 164.504(e)(2).
\textsuperscript{22} GAO REPORT, supra note 1, at 12-13.
\textsuperscript{23} \textit{Id.} at 16-17. \textit{See also} 45 C.F.R. § 164.512(i) (research provisions).
\textsuperscript{24} GAO REPORT, supra note 1, at 17. \textit{See also} 45 C.F.R. § 164.520 (access provisions).
\textsuperscript{25} GAO REPORT, supra note 1, at 19-20. \textit{See also} 45 C.F.R. § 164.520-.528 (patients’ rights provisions).
\textsuperscript{26} GAO REPORT, supra note 1, at 20-21.
2004). Many covered entities dreaded the compliance date for the privacy rule for fear of incurring significant criminal and civil sanctions for accidental or incidental privacy violations.

More specifically, between April 14, 2003, and April 14, 2004, consumers and other individuals filed 5,648 privacy-related complaints with the OCR. OCR closed approximately one-half of these complaints by May of 2004. Approximately 56% of these complaints related to inappropriate uses and disclosures of patient information, approximately 33% related to inadequate safeguards for patient information, and approximately 17% percent reported problems with patients gaining access to their own information. The OCR found that the majority of complaints (over 79%) were not germane to the privacy rule because either: (1) the complained of action was not prohibited by the privacy rule (35.4%); (2) the entity cited in the allegation was not a covered entity to which the rule applies (17.7%); or (3) the alleged action occurred before the compliance date (9.6%). Of the 21% of complaints that were germane to the privacy rule, OCR determined that a violation occurred (and the OCR was able to obtain the entity’s agreement to corrective action) in 9.4% of cases, and that no violation occurred in the remaining 11.5% of cases.

---

27 Id.
28 Id. at 20.
29 Id.
30 Id. at 21.
31 Id.