Engelberg Center for Health Care Reform at Brookings

FDA Sentinel Initiative Meeting Series

ISSUE BRIEF

Legal Issues in Active Medical Product Surveillance March 2010

PANEL 2
Protecting Patient Privacy in Medical Product Safety Surveillance

Deven McGraw, Health Privacy Project, Center for Democracy & Technology
Kristen Rosati, Coppersmith Schermer & Brockelman PLC

INTRODUCTION - FDA'S SENTINEL INITIATIVE

Consistent with its mission to protect and promote the public health, the Food and Drug Administration (FDA) launched the Sentinel Initiative to create the Sentinel System, an electronic system operating across different data sources—provider electronic health records, health plan claims databases, Medicare databases, and other data sources—to monitor medical products approved by the FDA. FDA plans to use the Sentinel System to strengthen its ability to monitor the performance of medical products after approval and improve its current drug and medical device safety surveillance capabilities.

This work is in alignment with the Food and Drug Administration Amendments Act of 2007 (FDAAA). Section 905 of this statute calls for the Secretary of Health and Human Services (HHS) to develop methods to obtain access to disparate data sources and to establish an active post-market risk identification and analysis system that links and analyzes healthcare data from multiple sources.[1] The law sets a goal of access to data from 25 million patients by July 1, 2010, and 100 million patients by July 1, 2012.[2] The law also requires FDA to work closely with partners from public, academic, and private entities.[3]

The FDA initially will implement the Sentinel System using existing external data sources, who will perform the safety analyses on health data they maintain and report back to the FDA (or to entities contracted to FDA to perform work on the agency's behalf consistent with its mission) aggregate data in response to drug and device safety questions.[4] FDA initially envisioned Sentinel as involving the gathering of only "de-identified" data.[5] However, it is possible that even in the earliest phase of the Sentinel Initiative, the aggregate data needed to address a particular query may not technically be de-identified and thus may qualify as identifiable under the Health Insurance Portability and Accountability Act (HIPAA).[6] Others hope that the data "pathways" used for the Sentinel System can be utilized in the near future for public and private sector research that is not controlled by, or even directly related to, FDA's mission.

Of utmost concern to FDA and the public is that the Sentinel Initiative is structured in a way that secures and maintains the public's trust and complies with existing federal and state laws protecting the privacy, confidentiality, and security of health information. In general, Americans support having their health information utilized to promote public health; but they also have significant concerns about the privacy of their health information.[7] Legal experts have analyzed the legal issues that arise with respect to access to data by FDA and its contracting partners for the earliest phases of the Sentinel Initiative.[8] This issue brief is not intended to be a substitute for the comprehensive legal analysis offered therein. Analysis of later

phases that might involve participants beyond the FDA and for purposes beyond post-market surveillance has not been completed and is beyond the scope of this issue brief. Instead, this brief summarizes applicable federal privacy laws that apply to FDA's initial implementation plans for the Sentinel System and raises some additional issues that will need to be resolved as the Sentinel System is implemented.

PRIVACY LAWS COVERING SENTINEL

In the initial phases of the Sentinel Initiative, data sources will not release fully individually identifiable information to FDA or its partners for analysis but will instead run product safety queries internally in their systems and report back aggregate results. The FDA (and its partners acting on its behalf) is legally authorized to both pose the queries and receive the aggregate data in response under the FDAAA. As explained in more detail below, federal law allows data sources to run the queries and release aggregate data to the FDA and its partners in response without the need to obtain consent or authorization from individuals.[9] (State law may place more stringent requirements on a data source's ability to internally analyze data for, and send an aggregated response to, the FDA; an analysis of those laws is beyond the scope of this brief.)

Authority for Access and Use of Data by Entities Serving as Sentinel Data Sources

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) and its regulations (primarily for purposes of this brief, the Privacy and Security Rules) present the most obvious federal requirements that apply to the use of health information for product safety analyses.[10] Many anticipated data sources for the Sentinel Initiative likely will be HIPAA covered entities – health systems, hospitals, other health care providers that have treatment relationships with individuals, and health plans (including the Medicare program and private health plans).[11] Others, such as health information exchanges, could be business associates and also must comply with HIPAA.

An analysis of whether HIPAA permits covered entities to participate in the Sentinel Initiative is in two parts: (1) does the authority exist for the entity to internally access and use identifiable health information (otherwise known as protected health information or PHI) to run Sentinel product safety queries; and (2) does the authority exist for disclosure of the aggregate data to the FDA and its partners in response to those queries.

The first part of the analysis involves the data sources' authority under HIPAA to *internally* access and use health information to run product safety queries on behalf of FDA and its partners. HIPAA rules permit covered entities to internally use individually identifiable health information for product safety analysis under the "public health," "health care operations," and "research" provisions of the HIPAA privacy regulations.

As discussed in more detail below, the HIPAA Privacy Rule permits covered entities to *disclose* identifiable health information for certain public health purposes.[12] While the HIPAA Privacy Rule provision on public health does not expressly cover an entity's internal access or use of the information,[13] the Rule mostly likely would treat an entity's internal use of PHI as a contracting partner to the FDA as a permissible public health purpose.[14] Where the data source is serving only as a data source and is not under contract to the FDA to perform analyses for purposes of Sentinel, this public health exception would not apply. However, in such a case the covered entity could rely on the "health care operations" provisions of the Privacy Rule to access and use the data to perform analyses for the Sentinel Initiative.[15] Health care operations, which may be performed without patient consent, include "population-based activities

relating to improving health."[16] Population-based activities are not defined in the Privacy Rule, but the Preamble to the Rule indicates that an analysis applied across an entire patient population that does not result in the treatment of an individual may be treated as population-based activities.[17]

In addition, where the HIPAA public health exception does not apply to internal access or use of information for purposes of the Sentinel Initiative, the exception for research may apply. Research using identifiable health information can be conducted without individual authorization under certain circumstances, including when the need for consent is waived by an IRB or a Privacy Review Board.[18]

Business associates, which contract with covered entities to perform functions on the covered entity's behalf using health information,[19] are also required to comply with most HIPAA regulations. Business associates may perform data analysis for Sentinel if it is consistent with their business associate agreements with covered entities. Some have suggested that Health Information Exchanges (HIEs) that are being created at the national, state and local levels could be potential data sources for the Sentinel Initiative. In the HITECH provisions of the American Recovery and Reinvestment Act of 2009 (HITECH), Congress deemed HIEs to be business associates under HIPAA; thus the ability of an HIE to access and analyze data for the Sentinel Initiative will depend on its contracts with the covered entities that form the HIE. [20]

Two other provisions of the HIPAA regulations are worth noting: the "minimum necessary" standard under the Privacy Rule and the HIPAA Security Rule. Covered entities and business associates are required to comply with HIPAA's "minimum necessary" provisions in the use and most disclosures of PHI (except for treatment disclosures). This simply means that an entity must make reasonable efforts to limit the information to the minimum amount of information that is necessary to accomplish the intended purpose of the use, disclosure, or request,[21] with some limited exceptions.[22] Under HITECH, covered entities must use a HIPAA limited data set (information stripped of "direct" patient identifiers that is still considered to be identifiable) or de-identified data to meet the minimum necessary standard if it is feasible to do so.[23]

HIPAA covered entities also must follow the HIPAA Security Rule with respect to the handling of identifiable health information. In summary, the Security Rule requires administrative, technical, and physical security safeguards to protect health information in electronic form.[24] Business associates also are now required to comply with most of the requirements of the security rule.[25]

Other Federal Requirements

Some data sources for the Sentinel Initiative may be covered by the federal regulations governing alcohol and drug abuse treatment information (commonly referred to as the "Part 2 regulations"). [26] These regulations permit internal access and use on a "need to know" basis [27] and so would not limit the internal use of this information for Sentinel analysis.

Authority for Release of Aggregate Data to FDA and its Partners

FDA and its contracting partners are seeking aggregate data in response to product safety queries. Initially the agency assumed that much of this data would be "de-identified" according to HIPAA standards.[28] However, as the FDA has begun to roll-out the Sentinel Initiative, it has become increasingly apparent that even in the earliest phases of Sentinel the aggregate data needed to address a particular query may not technically be "de-identified" and thus may qualify as identifiable under HIPAA.[29] Consequently, Sentinel data sources will need legal authority to *disclose* some identifiable data without individual patient authorization to the Sentinel coordinating center.

The FDAAA expressly prohibits FDA and its collaborative partners from disclosing "individually identifiable health information when presenting …drug safety signals and trends or when responding to inquiries regarding such drug safety signals and trends."[30] However, legal experts have concluded that this provision is intended to prohibit FDA and its collaborative partners from releasing individually identifiable information to third parties – and should not be read to prohibit a data source from releasing aggregate but still identifiable information to the FDA or its partners, as long as it is done in compliance with HIPAA.[31]

The federal privacy laws governing release of information to FDA and its partners distinguish between data that is "de-identified" and that is identifiable or potentially identifiable. The federal legal authority governing disclosure to FDA and its partners of both types of data is discussed further below.

HIPAA: De-identified Data

Data that meets the definition of "de-identified" under the HIPAA regulations is not regulated by HIPAA, which covers only individually identifiable health information.[32] Consequently, there are no legal impediments under HIPAA for covered entities to send de-identified data to the FDA and its partners. Data is de-identified if there is a very small risk of re-identification, and the Privacy Rule provides two methods for de-identification. The first, called the statistical method, involves the use of a qualified statistician to determine and document that the data presents a very small risk of re-identification.[33] The second, called the safe harbor method, requires the removal of 18 specific data points, including name, date of birth, date of medical service, most location data, and other identifying information such as a patient ID number or identification code.[34] As noted above, once information is "de-identified" according to HIPAA standards, it is no longer subject to HIPAA – which means entities are not legally required to abide by either the Privacy Rule or the Security Rule when disclosing it. However, data sources would be wise to apply security protections to data submitted to FDA and its partners even when the data is in de-identified form.

HIPAA: Aggregate but Potentially Identifiable Data

Data that is aggregated but technically not de-identified is considered identifiable. The HIPAA Privacy Rule permits covered entities to disclose individually identifiable (or "protected") health information (PHI) for a variety of public health purposes,[35] two of which may apply in the context of the Sentinel Initiative. First, HIPAA permits a covered entity to release PHI to a public health authority – including the FDA - who is authorized by law to receive the information for a public health purpose.[36] This provision also allows the release of such data to a person or entity acting under a grant of authority from or under contract with the FDA.[37] Second, the HIPAA Privacy Rule also permits disclosure to a person or entity that is subject to FDA's jurisdiction "with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity," including to "conduct post marketing surveillance."[38] This provision allows the release of PHI for surveillance to the FDA, its contracting partners, and to the manufacturer of the product under surveillance or investigation.[39] The HIPAA Privacy Rule also permits disclosure of PHI for "research" purposes, which is discussed in a separate Issue Brief.

The HIPAA Security Rule and the HIPAA "minimum necessary" standard, also discussed above, would apply to the disclosure of potentially identifiable data to FDA and its partners. Business associates (such as HIEs) would be permitted to disclose PHI for Sentinel to the extent permitted by their contracts with covered entities and pursuant to the same HIPAA rules governing covered entities.

Other Laws Relevant to Disclosure of Aggregate but Potentially Identifiable Data

The federal rules governing alcohol and drug abuse treatment information – the Part 2 regulations – are more stringent with respect to disclosure of identifiable data (data that is de-identified is not covered by Part 2).[40] Part 2 applies to federally assisted substance abuse treatment programs and entities that receive information from such programs. [41] The Part 2 regulations place substantial restrictions on the use and disclosure of identifiable information; however, they apply only to information that expressly or impliedly identifies a patient as an alcohol or drug abuser or someone who has applied for or received drug or alcohol treatment.[42] Thus, as long as the information disclosed as part of the Sentinel Initiative does not identify an individual as a substance abuser, the data can be disclosed to FDA and its partners for product safety surveillance.

Other federal laws that may apply to some data sources do place some limits on the disclosure of identifiable information, but none appear to impose limitations that would frustrate the goals of the initial phases of Sentinel.[43]

State health information confidentiality laws do place some limits on information disclosure, and most apply to certain types of sensitive information such as genetic information, HIV testing information, and mental health data. An analysis of those laws is beyond the scope of this brief. Data sources for Sentinel will need to carefully analyze any applicable state law.

CONCLUSION

The creation of a distributed data network that leaves individually identifiable data at the data source, versus creating a centralized database for analysis, alleviates many of the legal risks that might otherwise create obstacles to the sending of aggregate analyses to the FDA or its partners as part of Sentinel. At the federal level, legal authority exists to allow data sources to analyze health information they maintain for product safety signals. With respect to transmitting aggregate data to FDA and its Partners in response to safety queries, federal laws largely authorize such transmission – but the source and scope of that authority varies somewhat depending on whether or not the data qualifies as "de-identified" under the HIPAA Privacy Rule. Notwithstanding the distinction in privacy laws between de-identified and identifiable data, federal laws do not present any significant obstacles to the early phases of Sentinel, and the implementation pathways are relatively clear. Although the greatest amount of legal discretion with respect to data transmission exists if the data qualifies as de-identified, the disclosure of de-identified data does not alleviate all privacy concerns. Serious questions have been raised about whether the current HIPAA de-identification standard is sufficiently robust to protect data from re-identification.[44] Consequently, to build public trust in Sentinel, FDA, its collaborative partners, and Sentinel Initiative Data Sources should treat all information as potentially re-identifiable and protect it with reasonable security protections. They also should employ strong data use agreements to limit the use of data to the Sentinel Initiative.

---

[1] Food and Drug Administration Amendments Act of 2007, Pub. L. No. 110-85, § 905(a), *adding* Federal Food, Drug, and Cosmetic Act § 505(k), *amending* 21 U.S.C.A. § 355 (FDAAA).
[2] FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(B)(ii)(I)-(II)..
[3] FDAAA § 905(a), 21 U.S.C.A. § 355(k)(3)(B).
[4] Kristen Rosati, An Analysis of Legal Issues Related to Structuring FDA Sentinel Initiative Activities, eHI Health Initiative Foundation (March 2009), at http://www.ehealthinitiative.org/sites/default/files/file/eHealth%20Initiative%20Sentinel%20System%20Legal%20Guidance--%20Developed%20by%20Coppersmith%20Gordon%20(final).pdf (Rosati 2009).

[5] Rosati 2009 at 7; see also U.S. Dept. of Health and Human Services, Food and Drug Administration (FDA), The Sentinel Initiative (May 2008), at http://www.fda.gov/downloads/Safety/FDAsSentinelInitiative/UCM124701.pdf (FDA Sentinel Initiative 2008)
[6] Rosati 2009 at 15.
[7] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006); National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).
[8] Rosati 2009; see also Barbara J. Evans, Congress's New Infrastructural Model of Medical Privacy, 84 NOTRE DAME LAW REVIEW 585-654 (2009) (Evans 2009)
[9] Obtaining lawful authorization from the individual is arguably the certain way to legally access, use or disclose that individual's health information, but we presume that such a legal pathway is not feasible for conducting the Sentinel Initiative, given the number of records needed to accurately conduct postmarket surveillance.
[10] Section 905 also expressly requires Sentinel to be in compliance with HIPAA regulations. FDAAA §905(a), 21 U.S.C.A. § 355(k)(3)(C)(i)(I).
[11] Rosati 2009 at 8; see also 45 C.F.R. § 160.102.
[12] 45 C.F.R. § 164.512(b)
[13] Id.
[14] See Evans 2009 at 617.
[15] Rosati 2009 at 16-17.
[16] 45 C.F.R. §164.501.
[17] 65 Fed. Reg. 82,626 (Dec. 28, 2000).
[18] Cite to HIPAA research rules
[19] 45 C.F.R. § 164.103.
[20] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, §13408 (ARRA).
[21] 45 C.F.R. § 164.502(b)(1).
[22] 45 C.F.R. § 164.502(b)(2) (exceptions for disclosures to a health care provider for treatment; to the individual of his or her own information, or where the disclosure to a third party is requested by the individual; pursuant to an authorization; to the Secretary of HHS to investigate compliance with the Privacy Standards; as required by law; and as required for compliance with the Privacy Standards).
[23] ARRA § 13405(b)(1)(A).
[24] 45 C.F.R. Part 164, Subpart C.
[25] They must comply with sections 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies and procedures and documentation requirements) of title 45, Code of Federal Regulations. ARRA.§13401
[26] Rosati 2009 at 22.
[27] 42 C.F.R. §§ 2.1 through 2.67.
[28] Rosati 2009 at 7; see also FDA Sentinel Initiative 2008.
[29] For example, if the amount of data in the aggregate data is too small to qualify as presenting a very small risk of re-identification, the data does not qualify as "de-identified" and therefore must be treated by HIPAA-covered data sources as identifiable, even if neither the FDA nor its contracting partners can specifically identify the individuals whose data is involved. [Is this an appropriate way to characterize one of the key problems – the small cell problem?] Yes
[30] FDAAA §905(a), 21 U.S.C.A. § 355(k)(4)(B).
[31] Rosati 2009 at 47; Evans 2009 at 602-3.
[32] 45 C.F.R. §164.514(a)
[33] 45 C.F.R. § 164.514(b)(1)
[34] 45 C.F.R. §164.514(b)(2)(i)
[35] 45 C.F.R. §164.512(b).
[36] 45 C.F.R. §164.512(b)(1)(ii).
[37] A public health authority is, "an agency or authority of the United States…or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agenct of public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." 45 C.F.R. § 164.501
[38] "[T]he Privacy Rule specifically permits covered entities (such as pharmacists, physicians or hospitals) to report adverse events and other information related to the quality, effectiveness and safety of FDA-regulated products both to the manufacturers and directly to FDA." *See* http://www.fda.gov/Safety/MedWatch/HowToReport/ucm085589.htm (citing HHS Office for Civil Rights Guidance Explaining Significant Aspects of the Privacy Rule at page 28; see also 45 C.F.R. 164.512(b)(1)(i) and (iii))
[39] Rosati 2009 at 53.
[40] Rosati 2009 at 59.
[41] 42 C.F.R. §§2.3, 2.11.
[42] U.S. Dept. of Health and Human Services, Substance Abuse and Mental Health Services Administration, The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs" (June 2004), at http://www.hipaa.samhsa.gov/download2/SAMHSAHIPAAComparisonClearedPDFVersion.pdf.
[43] Rosati 2009 at 59-63.

[44] Center for Democracy & Technology, Encouraging the Use of, and Rethinking Protections for De-identified (and "Anonymized") Health Data (June 2009), at http://www.cdt.org/files/pdfs/20090625_deidentify.pdf; see also Paul Ohm, Broken Promises of Privacy: Responding to the Suprising Failure of Anonymization (August 2009), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006; Bradley Malin and Latanya Sweeney, How (Not) to Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification to Evaluate and Design Anonymity Protection Systems, Journal of Biomedical Informatics 37(2004), 179-192; Latanya Sweeney, Computational disclosure control, a primer on data privacy protection (2001), at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf .