

Engaging Patients: Building Trust and Support for Safety Surveillance

June 23, 2015

Discussion Guide

Introduction and Workshop Context

The rapid identification of adverse events related to medical products is of paramount concern to the U.S. Food and Drug Administration (FDA), patients, providers, and manufacturers of the product. The speed of identification depends on effective data systems and methods of analysis to quickly make a regulatory or health care decision in response to the adverse event. To complement existing passive surveillance systems, the FDA launched the Sentinel Initiative to establish a postmarket risk identification and analysis system, the Sentinel System, that links and analyzes safety data from multiple sources in, or near, real time.

The Sentinel System—a state of the art active surveillance data infrastructure—relies on a distributed data architecture to rapidly scale analysis of health care data collected from over 178 million patients nationwide. Already a proven and effective surveillance tool for FDA, it is being increasingly recognized as the basis for a national resource to support the needs of diverse stakeholders including other public health agencies, health systems, regulated industry, and the clinical research enterprise. However, despite Sentinel’s demonstrated successes and opportunities to further improve health outcomes, patients are largely unaware of Sentinel’s public health mission and commitment to protecting patient privacy. Therefore, it is both timely and critical to identify opportunities to raise awareness and build trusted support for Sentinel between patients, consumers, and the general public.

The continued success of Sentinel will depend not only on maintaining strong stakeholder and public confidence but developing meaningful partnerships based on trust. While many opportunities exist, the focus of this workshop, which builds on meetings previously convened by FDA and Brookings, will explore strategies for how Sentinel Data Partners and third party organization can facilitate effective Sentinel communication to patients. Three primary questions will be considered:

- 1) How can Sentinel Data Partners leverage experience using existing mechanisms for patient outreach to communicate about Sentinel?
- 2) What information could be communicated to patients about Sentinel that will raise awareness and build broad support?
- 3) Are there best practices or promising mechanisms that could be shared by third party organizations to either inform or complement Sentinel Data Partner communications about Sentinel to patients?

This discussion seeks to generate principles for strategic messaging of Sentinel and opportunities to maximize impact of this message leading to a set of actionable recommendations for Data Partners and stakeholders to consider for implementation within their organizations. Ultimately, through more effective communication it is anticipated that patients will not only have an increased awareness of Sentinel’s value and understanding of how this system directly improves their health but could also be motivated to further explore and engage with other public health initiatives like Sentinel that support population health.

What is Safety Surveillance and How Does FDA Conduct Surveillance Activities?

Patients and consumers routinely encounter a variety of medical products, including drugs, biologics, vaccines, devices, diagnostic tests, etc., in the delivery of care. At the time of approval, a medical product has been shown to have benefits that outweigh the potential risks. As data accumulates throughout the lifecycle of a medical product new information is revealed on both performance and its safety profile. For instance, drugs approved based on clinical trial data have been tested in a relatively small and carefully selected population of patients, which may differ from the broader population of patients who will take the drug once it is approved. Further, clinical trials are unlikely to detect rare adverse events because of the limited population enrolled. As such, many important safety concerns may arise in the postmarket environment. To monitor these concerns, the FDA relies on multiple data sources including relevant medical literature, postmarket safety studies, and analysis of reports of suspected adverse drug reactions and medication errors.

Each center at FDA has systems in place to capture reported adverse events by regulated industry, which are bulleted out below. In addition to this mandatory reporting by industry, FDA receives voluntarily submitted reports from health care professionals and consumers (i.e., patients, family members, caregivers) through FDA's MedWatch of suspected adverse drug reactions and medication errors.

- The FDA Adverse Event Reporting System (FAERS), a database that captures reports of adverse events related to prescription drugs (CDER) and therapeutic biologic products. (CBER)
- The Vaccine Adverse Event Reporting System (VAERS), a database that captures reports of suspected vaccine-related adverse reactions. (CBER)
- The Manufacturer and User Facility Device Experience (MAUDE) captures reports of suspected medical device related adverse reactions. (CDRH)

Once a safety concern is identified, the FDA has numerous mechanisms in place to communicate this new information about the medical product. This may include a product labeling change or a range of safety communications posted on FDA's website and disseminated through FDA's MedWatch program. In addition, manufacturers, insurers, and medical professionals may also be disseminators of this information by notifying patients and consumers through informational packets such as patient medication guides or other correspondence to convey emergent risks that may necessitate prompt medical attention.

While passive surveillance techniques, which rely on the submission of reports by manufacturers or the public, are the historical norm for safety surveillance, there is increasing need and capacity to more quickly identify adverse events. Active surveillance involves the use of electronic health care data in, or near, real time to identify potential safety signals not reported through traditional surveillance systems. Use of this electronic data allows the FDA to rapidly evaluate and understand a safety issue in greater depth, for example, through targeted analysis of patient subgroups (e.g., age and gender). Both active and passive surveillance techniques have an important, complementary role in safety surveillance and provide the FDA with different tools to comprehensively monitor medical product safety. To this end and to build the necessary data infrastructure for active surveillance, the FDA launched the Sentinel Initiative.

Sentinel System Overview

The Sentinel Initiative represents an active component of FDA's postmarket surveillance systems, augmenting surveillance data of regulated products reported voluntarily by manufacturers, clinicians,

and patients regarding adverse outcomes, quality issues, and other factors observed from treatments. Building on pilot efforts to conduct active postmarket surveillance, including systems like the Centers for Disease Control and Prevention's (CDC) Vaccine Safety Datalink, FDA formally established the Sentinel Initiative in response to the Food and Drug Administration Amendments Act (FDAAA) of 2007. Since then, the Sentinel Initiative has grown from an early pilot program, the Mini-Sentinel pilot, to a core surveillance program at FDA to provide evidence on an increasing range of safety questions. Key features of the Sentinel System's safety surveillance include:

- Capacity to assess outcomes that are reliably captured in electronic claims data (e.g., hospitalizations, procedures)
- Capacity to identify use of specific brand and generic drugs dispensed in ambulatory settings that are reimbursed by health plans (some inpatient administration)
- Accessible denominators to calculate rates of adverse events and other treatments and outcomes
- Large sample sizes for population subgroup analysis

An Overview of Sentinel's Distributed Data Architecture and Process for Analysis

The Sentinel System, which is based on the Mini-Sentinel pilot, uses a distributed data approach in which Sentinel Data Partners¹ maintain physical and operational control over their electronic health care data in their existing environments (i.e., behind their respective firewalls). Once a safety question is prioritized, the FDA in partnership with the Sentinel Operations Center (SOC) develops standardized data queries, which are then distributed to Data Partners for analysis. The output of these queries, typically in summary form, are then provided back to the SOC. Harvard Pilgrim Health Care Institute is currently serving as the SOC. This process is visually depicted in Figure 1 below. The key to scalability is the use of the Sentinel Common Data Model (CDM).

The CDM makes it possible to execute standardized programs developed by the SOC by allowing Data Partners to maintain and access data in a common data format. The CDM relies on existing standardized coding schema (e.g., ICD-9-CM, HCPCS/CPT, and NDC) to minimize technical challenges with interoperability and is continuously being maintained, updated and enhanced by the SOC. The CDM was built based on the data elements found in electronic health care data from Data Partners, which includes administrative claims data, some outpatient and inpatient electronic health records, demographic information, outpatient pharmacy dispensings, and registry data.

Sentinel Data Partners adhere to all privacy provisions that the Health Insurance Portability and Accountability Act (HIPAA) prescribes for public health activities.² In addition, the Office for Human Research Protections has determined that the regulations administered by that office (45 CFR part 46) do not apply to the activities under FDA's Sentinel Initiative. Therefore, the work of Sentinel is not reviewed by Institutional Review Boards (IRB).³

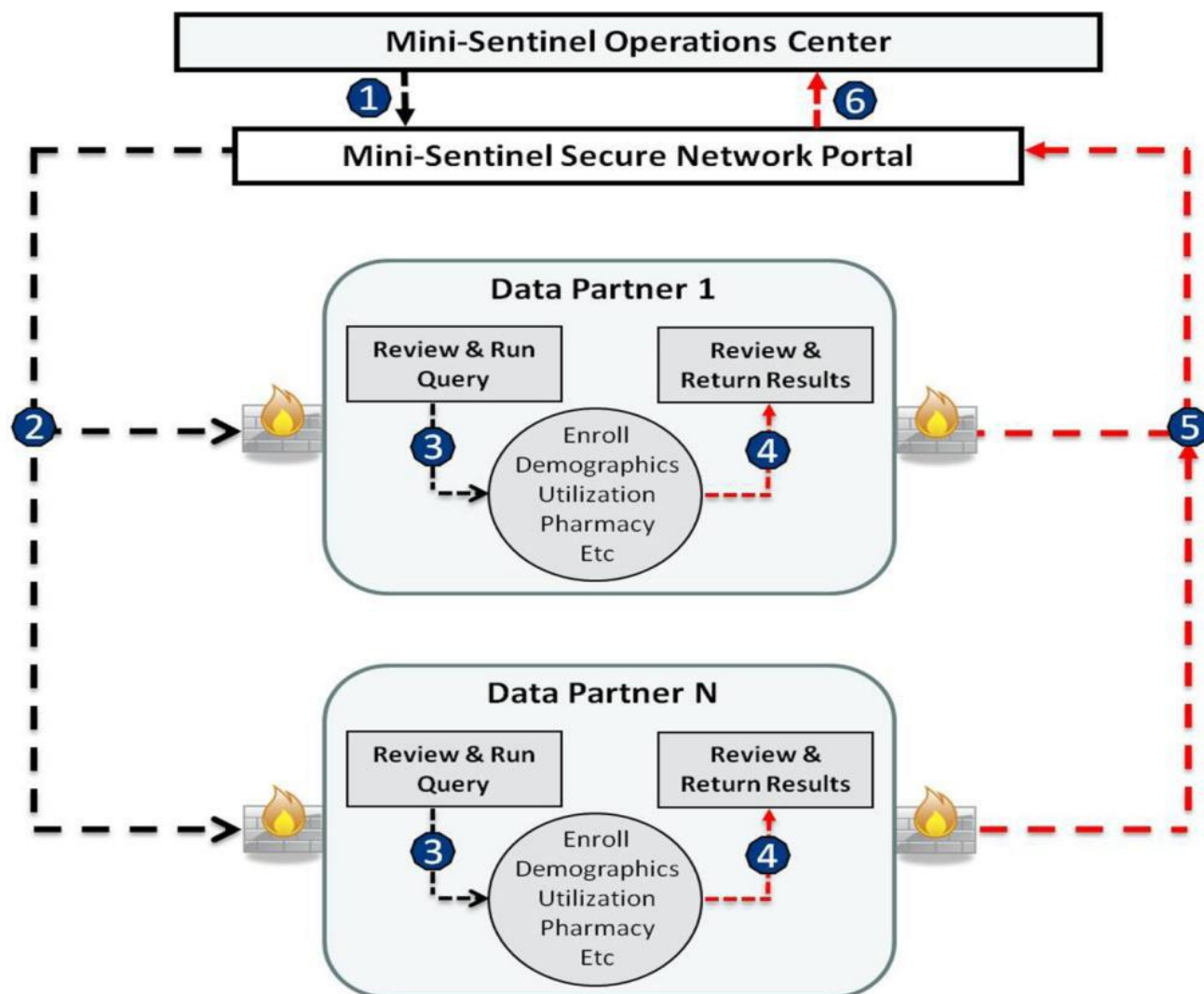


Figure 1. Overview of Mini Sentinel Distributed Network. (Source: Dr. Richard Platt, Harvard Pilgrim Health Care Institute).

Importance of Communication in Safety Surveillance

As technology evolves, there are more opportunities to connect patients to the health care system. The development and widespread use of electronic health records and patient portals, for example, are providing new opportunities to facilitate this communication between patients and providers. There is also interest in bridging the gap between patients and the clinical research enterprise. The National Patient-Centered Clinical Research Network (PCORnet) is a unique initiative intended to develop specific opportunities for patient involvement and activation in clinical research.⁴ Initiatives like PCORnet, which share a similar distributed data architecture and CDM with Sentinel, provide an opportunity to link these distributed networks with the Sentinel System forming a national resource to generate other forms of evidence development. As this evolution continues, it will be important for patients, health care

providers, regulators, industry, and other stakeholders to not only be aware of the Sentinel System but provide concrete opportunities for engagement that build strong public confidence through trusted partnerships and transparency in its use.

Workshop Rationale

In support of FDA's commitments to transparency and active engagement with stakeholders in Sentinel, Brookings convened an expert workshop in 2012 focusing on patient and consumer engagement in the Sentinel Initiative. The workshop was designed to provide patient and consumer advocates with an overview of the Sentinel Initiative, open a dialogue on opportunities for further patient and consumer engagement opportunities, and identify concrete next steps for expanding engagement. Discussions from the 2012 workshop uncovered a number of recommendations on how to engage patients and consumers, including:

The need to communicate about the Sentinel System: FDA inquired about the type of information that would be most valuable to patients. Participants suggested sharing updates on Mini-Sentinel development, providing explanations of Mini-Sentinel in layman's terms, and the roles, if any, of third party organizations.

The spectrum of patient and consumer information needs: The amount of information patients and consumers require about their medication varies; some may desire only actionable information while others desire a broader net of information including rationale for regulatory decision-making. The Mini-Sentinel Website can be the vehicle for sharing information in a format friendly to the public for broad patient information needs with an emphasis for patients/consumers on its public health mission and commitment to protecting patient privacy.

Expressed interest in increasing public awareness of Sentinel and safety surveillance. Both participants and the FDA expressed interest in continuing to engage patients and consumers to keep them abreast of, and ways to involve them in, Sentinel activities.

Building on these recommendations, the current expert workshop "Engaging Patients: Building Trust and Support for Safety Surveillance," aims to engage representatives from the FDA, Sentinel Data Partners, patient and consumer advocacy organizations, and experts in patient privacy, ethics, and health literacy, to share, learn, and develop strategies for delivering well framed messaging of Sentinel to patients. Since Sentinel Data Partners have direct relationships with patients that participate in their health plans, there could be opportunities to leverage this relationship to improve Sentinel communication and maximize the impact of messaging to patients. To begin identifying these opportunities this workshop is organized with the following objectives, which will facilitate the day's discussion:

- Present Sentinel Data Partner experiences in member outreach with the aim of identifying best practices and key barriers to communication. A patient representative will comment on how information is currently communicated to patients.
- Develop guiding principles for communicating information of meaning and value about Sentinel to patients and how to strategically frame the message to prevent misperceptions of privacy concerns and use of health information within the Sentinel System.
- Explore innovative practices or promising mechanisms currently used by advocacy organizations and how these mechanisms could support or complement Sentinel Data Partner communications.

The goal is to not only raise awareness of Sentinel among patients but also build trust and broad support for participation in similar initiatives focused on population health. Meaningful engagement with

patients is critical to this aim, and the actionable strategies identified during this workshop will represent a tangible step forward on this important topic.

¹ The most recent published list of Sentinel Data Partners can be viewed at: http://www.mini-sentinel.org/about_us/collaborators.aspx.

² For more information on HIPAA requirements, please review: <http://www.hhs.gov/ocr/office/>

³ For more information about Sentinel's HIPAA and Common Rule Compliance, please review Rosati, Evans and McGraw's white paper entitled, "HIPAA and Common Rule Compliance in the Mini-Sentinel Pilot." (http://www.mini-sentinel.org/work_products/About_Us/HIPAA_and_CommonRuleCompliance_in_the_Mini-SentinelPilot.pdf)

⁴ For more information on PCORnet see: <http://www.pcornet.org/>