MEDICAL COUNTERMEASURE SURVEILLANCE

USE OF MINI-SENTINEL CAPABILITIES TO IMPROVE MEDICAL COUNTERMEASURE SAFETY SURVEILLANCE

Prepared by: Gretchen Weiss, MPH,[1] Brooke Courtney, JD, MPH,[2] Matthew F. Daley, MD,[3] Arthur Davidson, MD, MSPH[4] Susan Forrow, BA,[5] Kristin Goddard, MPH,[3] Melissa McClung, MSPH,[4] Ted Palen, PhD, MD, MSPH,[3] Richard Platt, MD, MSc,[5] Raymond Puerini, MPH,[1] Kristen Rosati, JD,[6] Andrew R. Roszak, JD, MPA,[1] Marsha E. Reichman, PhD[7]

Author Affiliations: 1. National Association of County and City Health Officials, Washington, DC; 2. Office of Counterterrorism and Emerging Threats, Office of the Commissioner, FDA, Silver Spring, MD; 3. Institute for Health Research, Kaiser Permanente Colorado, Denver, CO; 4. Denver Public Health, Denver, CO; 5. Department of Population Medicine, Harvard Medical School and Harvard Pilgrim Health Care Institute, Boston, MA; 6. Polsinelli PC, Phoenix, AZ; 7. Office of Surveillance and Epidemiology, Center for Drug Evaluation and Research, FDA, Silver Spring, MD

September 27, 2015

Mini-Sentinel is a pilot project sponsored by the U.S. Food and Drug Administration (FDA) to inform and facilitate development of a fully operational active surveillance system, the Sentinel System, for monitoring the safety of FDA-regulated medical products. Mini-Sentinel is one piece of the Sentinel Initiative, a multi-faceted effort by the FDA to develop a national electronic system that will complement existing methods of safety surveillance. Mini-Sentinel Collaborators include Data and Academic Partners that provide access to health care data and ongoing scientific, technical, methodological, and organizational expertise. The Mini-Sentinel Coordinating Center is funded by the FDA through the Department of Health and Human Services (HHS) Contract number HHSF223200910006I. This specific project was funded by the Center for Drug Evaluation and Research (CDER) Task Order 7 (Contract number HHSF22301007T).

Medical Countermeasure Surveillance

Use of Mini-Sentinel Capabilities to Improve Medical Countermeasure Safety Surveillance

Table of Contents

I. INTRODUCTION

Medical countermeasures (MCMs) include both pharmaceutical MCMs, such as antimicrobials, antidotes, antitoxins, and vaccines, and non-pharmaceutical MCMs, such as ventilators, diagnostics, personal protective equipment, and patient decontamination that may be used to prevent, mitigate, or treat the adverse health effects of a deliberate, accidental, or naturally occurring public health emergency.[1] In response to a public health threat, such as a severe influenza pandemic or an aerosolized anthrax attack, MCMs may be used in support of treatment or prophylaxis to an identified population. Plans for stockpiling, distributing, and dispensing MCMs are largely coordinated by the U.S. Centers for Disease Control and Prevention (CDC) and by state and local public health agencies. Depending on the emergency and patient care needs, MCMs may be dispensed under a non-medical model (e.g., at points of dispensing (PODs) managed by local public health agencies) or through the traditional healthcare system (e.g., hospitals).

Though an extensive and growing framework exists for post-market safety surveillance of U.S. Food and Drug Administration (FDA)-regulated medical products, a more comprehensive and timely approach to monitoring and assessing the safety of drugs and vaccines administered as MCMs during emergencies is needed. This is particularly critical in situations when unapproved medical products are used as MCMs, or approved products are used in unapproved ways that may be authorized for emergency, such as in response to a rapidly emerging influenza pandemic. Also, some MCMs might have been approved using animal models and limited human efficacy testing, if broader human efficacy testing was not ethical or feasible. Therefore, timely data on the safety and efficacy of an MCM may be needed to help inform decision-makers and healthcare professionals about continued use of the MCM during the emergency response. Safety information also contributes to decisions about MCM use in future responses, as well as general post-market surveillance activities.

To conduct safety surveillance, receipt of the MCM, which may be delivered outside of the traditional healthcare setting, needs to be linked to potential adverse health outcomes, which are typically diagnosed and treated within the healthcare delivery system. This report will focus on MCMs dispensed outside of the traditional healthcare setting through local health department-run or -coordinated PODs and examine methods for linking externally collected data on receipt of the MCM to Mini-Sentinel health outcomes data (i.e., electronic healthcare data).

II. BACKGROUND

A. MCM DISTRIBUTION, DISPENSING, AND DATA COLLECTION AT PODS

Distribution and dispensing of MCMs in response to a public health emergency is a complex, interactive process that involves participation from all levels of government, as well as nongovernmental and civilian partners.[2] The Public Health Emergency Medical Countermeasures Enterprise (PHEMCE) is the coordinating body for the federal agencies charged with developing and utilizing MCMs to protect the U.S. civilian population during public health emergencies.[3] The PHEMCE is led by the U.S. Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness and Response and includes three HHS internal partners: CDC, FDA, and the National Institutes of Health, as well as several interagency partners: the Department of Defense (DoD), the Department of Veterans Affairs (VA), the Department of Homeland Security, and the Department of Agriculture. State, local, tribal, and territorial governments, public health systems, academia, private industry, and civilians are also critical to the success of ensuring that the United States is prepared to prevent, respond to, and reduce the adverse health effects of public health emergencies and disasters.[4]

Public health emergencies are primarily managed at the local level and local governments, in particular local health departments, play a lead role in local public health emergency responses.[5] Local health departments are responsible for developing and implementing plans to ensure that all potentially exposed individuals in their communities receive the appropriate MCM in accordance with public health and medical guidelines and recommendations. As laid out in CDC's *Public Health Preparedness Capabilities: National Standards for State and Local Planning*, this includes identifying and initiating MCM dispensing strategies; receiving MCMs; activating dispensing modalities; dispensing MCMs to an identified population; and reporting adverse events.[6]

The CDC plays a pivotal role in ensuring that state and local public health systems are prepared for public health emergencies. CDC's Office of Public Health Preparedness and Response (OPHPR), Division of State and Local Readiness administers funds for preparedness activities to state and local health departments through the Public Health Emergency Preparedness (PHEP) cooperative agreement. CDC also oversees the Strategic National Stockpile (SNS), which has caches of MCMs strategically located across the U.S. ready for deployment.[7] Once federal authorization is granted to deploy SNS assets, state and local authorities activate their MCM distribution and dispensing plans. Each state health department has plans to receive and distribute SNS assets to local health departments, and each local health department has plans to receive and dispense SNS assets to the local population. CDC's Cities Readiness Initiative (CRI) supports capacity building to deliver MCMs during a large-scale public health emergency.[8] CRI funds the nation's largest cities and metropolitan statistical areas to develop plans to quickly receive and distribute medicine and medical supplies from the SNS to local communities.

In some public health emergencies, MCMs may be managed and dispensed within the traditional healthcare system, such as in response to a single case of meningitis in a school. In other cases, the demand for MCMs may exceed the capabilities of what the traditional healthcare system can support, such as serial cases of meningitis at a university or a wide-area anthrax attack, when tens or even hundreds of thousands of individuals may need to receive MCMs within a short time period, or when limited supplies require controlled administration of MCMs to specific groups. In such cases, use of local, state, and/or regional MCM caches or the SNS is necessary, as well as the implementation of alternative methods to rapidly dispense MCMs to a large population.

One method for rapidly dispensing MCMs to a large population is through local health department-run or -coordinated PODs. PODs are mass dispensing sites capable of providing medications or vaccinations to a large number of people during a public health emergency. PODs typically employ either a "pull" or "push" mechanism. "Pull" mechanisms require the general public to come to PODs to pick up the MCM (e.g., drive-through clinics or clinics established at schools), whereas "push" mechanisms involve state and local officials sending the MCM to entities that are then responsible for delivering the MCM to specific populations (e.g., MCMs delivered to residences by school bus drivers).

PODs can be structured in a variety of ways:

Non-medical PODs provide care using a population approach (e.g., no individual medical examinations/assessments are conducted, rather brief screening algorithms are used to conduct assessments). This approach expedites MCM dispensing, while still assessing for the possibility of severe adverse reactions and maternal and child health considerations. To dispense the MCM, non-medical

PODs typically use trained staff or volunteers who are not licensed healthcare workers, in addition to licensed healthcare professionals.

Medical PODs are structured similarly to how medication is dispensed in routine patient care situations, using trained medical professionals to assess individual patients and dispense the MCM.

Open PODs are located within the community and are available to the public. Open PODs are managed by local health departments and typically staffed by trained volunteers from the community. There are several methods for delivery using this model. Some methods call for every individual receiving the MCM to visit the POD, such as mass vaccination clinics that require direct administration of the MCM. Other methods, such as Group and Head of Household, allow one individual to collect countermeasures from the POD and dispense the medication to others in the group or family.

Closed PODs dispense MCMs to a specific group, such as an organization, business, or university, under the local jurisdiction's official response plans, and are managed by the group's trained staff. This model differs from the open POD model, as it is not intended for the general public and does not require a representative from the group to visit an open POD to collect the MCM (as in the group model noted above, though closed PODs may employ the Head of Household approach, as well). In some cases, closed PODs may be opened to the public after all eligible individuals in the specific group receive the MCM. Pre-arrangements are made either for the local health department to deliver the MCM to the closed POD or for a closed POD representative to pick up the MCM from the health department. Local health departments work closely with these groups (e.g., businesses, universities) to ensure that they have the necessary resources and training.

Open and closed PODs are intended to be used in tandem during a public health emergency. Alternative and innovative models for MCM delivery are also continuously being explored. Many of these models use "push" mechanisms to deliver MCMs to individuals at their residences, such as using public school buses to deliver a supply of the MCM. MCM delivery methods rely, in part, on the type of MCM used. For example, the Head of Household and school bus models would not work if the MCM required administration by a trained professional or volunteer (e.g., a vaccine).

Individual level data (e.g., name, date of birth) for those receiving MCMs might be collected via POD processes. CDC's Public Health Preparedness Capabilities requires that jurisdictional plans include protocols to report aggregate data on those receiving the MCM to state/federal entities. Information on who received the MCM is also valuable to local public health and healthcare entities. Currently, the majority of jurisdictions across the country employ paper-based data collection methods and data collection plans are not designed to support linkage to electronic healthcare data (e.g., health insurance information is not collected). To improve safety surveillance for MCMs delivered via PODs, policies, processes, capabilities, capacities, and resources to support electronic data collection and linkage will need to be expanded. This will be explored further in Section III.

B. EXISTING SURVEILLANCE SYSTEMS FOR MEDICAL PRODUCTS

FDA and CDC lead efforts to monitor the safety and performance of deployed MCMs during and after an emergency response; however, the current systems are limited in their ability to rapidly and comprehensively monitor and assess the safety of MCMs dispensed in response to a public health emergency. In the U.S., reporting of adverse events and medication errors by healthcare professionals and consumers has historically been voluntary, except for specific adverse events that occur after the administration of routinely recommended vaccines. The federal government has established a number of voluntary (also referred to as spontaneous) reporting systems, which have served as the cornerstone of drug and vaccine safety monitoring. Additional surveillance systems have been developed to augment the data available through these voluntary reporting systems, including Mini-Sentinel. Over the past decade, there has been significant growth in the use of population-based active safety surveillance and epidemiological studies. “The overarching goal of these efforts is to expand and improve the use of currently available electronic healthcare data to increase the power, speed, and quality of safety monitoring after licensure.”[9]

The various systems that comprise the national safety surveillance framework differ mainly by data collection method (passive or active), access to patient medical records, and the underlying population size and characteristics.

1. Passive Adverse Event Reporting Systems

Passive systems rely on reports (often voluntary) of adverse events submitted from healthcare professionals, product manufacturers, and the public. These systems are the backbone of safety data collection for marketed medical products. Strengths of these systems include the ability to obtain national data (though the data cannot be assumed a representative sample, as it is primarily reported voluntarily), which can be used to rapidly detect increases in reports of adverse events following the use of specific products, to detect rare adverse events, and to generate hypotheses for further study. These systems may also be able to rapidly alert FDA and CDC of potential new safety signals. Weaknesses of these systems include subjectivity, underreporting, stimulated reporting (which may occur as a result of media attention on specific adverse events or public health interventions), variable data quality, and lack of denominator data, which limits the ability to determine incidence of adverse events and to conduct causality assessments. Furthermore, these systems are not designed to support linkage with MCM exposure data for the purpose of exposure-outcome assessments.

The FDA Adverse Events Reporting System (FAERS) contains information on adverse event and medication error reports that healthcare professionals and consumers submit to FDA. Healthcare professionals and consumers may also report adverse events and medication errors to the products’ manufacturers, who are required to send the report to the FDA. FAERS supports FDA's post-marketing safety surveillance program for drug and therapeutic biologic products and can assess early indicators of possible drug safety problems that may present as new or unusual adverse events or patterns.

The Vaccine Adverse Event Reporting System (VAERS) is a national vaccine safety surveillance program co-sponsored by FDA and CDC. VAERS collects information about adverse events that occur after the administration of vaccines licensed for use in the U.S. Anyone can file a VAERS report, including healthcare providers, manufacturers, and vaccine recipients.

2. Active Monitoring Systems

Active surveillance systems either actively collect primary data (e.g., via data abstraction, telephone interviews) or employ secondary use of electronic healthcare data from healthcare practitioners or insurance companies. During a public health emergency, active surveillance systems can augment existing passive systems. A key strength of these systems is the availability of denominator data, which supports the ability to detect and verify signals, assess the incidence of adverse events, and conduct causality assessments. Additionally, many active surveillance systems allow for near real-time collection and assessment of data.

The Vaccine Safety Datalink (VSD) provides a way of testing hypotheses generated through signal detection systems, such as VAERS. VSD is a collaborative effort between CDC's Immunization Safety Office and 10 managed care organizations (MCOs) to monitor immunization safety and address the gaps in scientific knowledge about adverse events following immunization. The VSD links computerized vaccination and medical records for approximately 9.2 million persons (3% of the total U.S. population) and has implemented a system to conduct near real-time (i.e., weekly) monitoring for specific adverse events in the VSD population. VSD is a highly developed federal vaccine active surveillance system, and can verify outcomes via access to full electronic medical records. However, it is limited in its abilities due to its population size, as well as its singular focus on vaccines.[10]

Mini-Sentinel is a pilot project sponsored by FDA to inform the creation of an active surveillance system – the Sentinel System – to monitor the safety of FDA-regulated medical products. FDA initiated the project in 2009 as part of its Sentinel Initiative, which was launched in response to the Congressional mandate in the FDA Amendments Act of 2007.[11] The Sentinel Initiative aims to develop and implement a proactive system that will complement existing systems that track reports of adverse events linked to the use of FDA-regulated products. The Mini-Sentinel is charged with developing the framework, data resources, analytic capabilities, policies, and procedures to satisfy this mandate.

Mini-Sentinel uses pre-existing electronic healthcare data from multiple sources (i.e., Data Partners). As of July 2014, there are 18 Data Partners, covering nearly 180 million individuals. Mini-Sentinel uses a distributed data approach in which Data Partners retain control over data in their possession. Data Partners transform local data into a common data structure according to the Mini-Sentinel Common Data Model (CDM) and execute standardized computer programs (i.e., queries), in response to FDA requests, within their own institutions, behind their firewalls. Aggregated results are shared with the Mini-Sentinel Operations Center (MSOC). If there is a need for person-level information, it is stripped of direct patient identifiers before being shared with MSOC. Aggregate data is then shared with the FDA for analysis. Mini-Sentinel is exploring a variety of approaches for improving the FDA's ability to generate, identify, and assess safety issues quickly.[12]

As the largest general population cohort available for active surveillance in the U.S., Mini-Sentinel has great potential to support MCM safety surveillance by providing health outcomes data for a large number of people across the country. Mini-Sentinel's large population size also permits stratified analyses that can potentially identify risks within subpopulations. Since use of electronic healthcare data does not rely on voluntary reporting, the data available through Mini-Sentinel provides a more complete account of health outcomes resulting from the administration of drugs and vaccines than voluntary reporting systems do, which expands decision-making capabilities during public health emergencies. Additionally, Mini-Sentinel provides a denominator for safety assessments, which can be used for determining incidence rates.

In order to conduct safety surveillance, medical product exposure data is needed. In the case of an MCM event, information concerning exposure to the MCM product may not be readily available in a timely fashion in the data routinely held by Mini-Sentinel's Data Partners as a result of normal course of business operations. For example, when the MCM is dispensed outside of the traditional healthcare setting (e.g., at a POD). Under this scenario, methods for making MCM exposure data available to Mini-Sentinel will be needed, which is discussed in detail in Section III.

While Mini-Sentinel has unique potential to support improved MCM safety surveillance, it is limited by the amount of time it takes for electronic healthcare data, and in particular administrative claims data, to stabilize and be available for query. Most Mini-Sentinel data are currently refreshed on a quarterly basis and contain relatively settled and complete data, the most recent of which are on average 6-9 months old. This timeframe does not adequately support decision making during or immediately following public health emergencies. Near real-time surveillance requires more frequent data updates and fresher data in each updated dataset. Efforts are underway to establish more timely access to fresher data, which is mentioned immediately below in the description of the Post-Licensure Rapid Immunization Safety Monitoring (PRISM) program and discussed further in Section III.

The PRISM program was created in 2009 by HHS to monitor the safety of the H1N1 influenza vaccine. To ensure its sustainability, PRISM was integrated into Mini-Sentinel in September 2010. The PRISM program created a distributed database that combined claims data from four national health insurers (all Mini-Sentinel Data Partners) with data from nine state immunization registries. PRISM is unique in its ability to capture data from sources outside traditional healthcare systems (e.g., immunization registries). However, PRISM is limited by how frequently the data is refreshed (PRISM data is only refreshed quarterly, consistent with the Mini-Sentinel's standard schedule; however, activities are underway to evaluate the feasibility of using fresher data available through more frequent refreshes);[13] its accessibility of medical records (PRISM's experience during H1N1 suggests that several months are needed to complete any desired review); and its focus on the study of a few specific vaccines.[14]

CDC's BioSense 2.0 is a public health surveillance system that operates as a collaborative data-exchange system that enables its users, who have agreed to share health data, to identify disease outbreaks and harmful health effects of hazardous agents and track them over time. The data available in BioSense 2.0 includes emergency department visits, hospitalizations, and other health-related data from multiple sources, including the VA, DoD, and civilian hospitals from around the country. BioSense 2.0 is the only public health surveillance system that enables state and local health departments and the CDC to quickly (data are refreshed daily) share emergency visit health information with each other across jurisdictional lines.[15]

An important use of the BioSense program is to identify public health emergencies for which MCMs might be used. BioSense has also been examined for its potential use to monitor and rapidly assess the safety of MCMs.[16] Findings suggest that BioSense data could be used to detect adverse events; however, since the system primarily provides aggregated data, the data alone cannot be used to identify individuals who have used MCMs and then identify health outcomes among those individuals. Linkage to MCM exposure would require extensive follow-back investigation for specific syndrome presentations. However, some jurisdictions have moved to individual, de-identified line-level data for emergency department admissions. As more jurisdictions expand this capability, and if emergency triage notes include words to identify exposure to the MCM, there could be increased potential for BioSense 2.0 to assess associations between MCM exposure and specified health outcomes.

Despite the availability and sophistication of these systems, capabilities to monitor and assess adverse events associated with MCMs used during a public health emergency remain limited, as evidenced by the MCM data collection and analysis challenges experienced during and after the 2009 H1N1 influenza pandemic.[17, 18, 19] The limitations include: operational challenges associated with surges in patient volume, staffing shortages, and insufficient pre-planning to address these circumstances; operational challenges that result from MCM dispensing practices (e.g., dispensing outside of the traditional healthcare setting, delivery speed, potential changes in standards of care); difficulty capturing individual identifiers for those receiving the MCM in a readily usable format (i.e., electronic) that supports linkage to electronic healthcare/health outcomes data; data sharing and linkage challenges due to lack of interoperability among existing surveillance and electronic healthcare information systems; and insufficient capabilities for timely data analysis during public health emergencies due to lag time associated with exposure and outcome data.

III. USE OF MINI-SENTINEL TO EXPAND MCM SAFETY SURVEILLANCE CAPABILITIES

To effectively monitor and assess the safety of a medical product, it is essential to have information on individuals receiving the medical product and health outcomes (i.e., diagnoses) for the same individuals, and to be able to link sources containing that data, if these differ. During a public health emergency, it is critical to be able conduct safety surveillance in a timely manner, as close to real-time as possible, so that safety problems can be detected and assessed in time to intervene. As previously discussed, the condensed timeframe and methods for MCM dispensing outside of the traditional healthcare setting present challenges to timely capture and use of MCM exposure data. Additionally, current data collection processes and existing surveillance systems are limited in their ability to support the requirements of MCM safety surveillance during public health emergencies. Recognizing these limitations, several efforts are underway to expand current capabilities and develop new mechanisms to establish a more comprehensive and timely approach to MCM safety surveillance.

While not all specifically focused on POD scenarios, federal efforts to strengthen and coordinate MCM surveillance capabilities include the PHEMCE MCM Monitoring and Assessment Integrated Program Team (IPT); the FDA MCM Adverse Events Monitoring and Analysis Pilot (MCM AE-MAP); and FDA's Mini-Sentinel pilot. The PHEMCE established an IPT to focus on developing capabilities for and coordination of MCM surveillance. The decision to establish the IPT was based on recognition of the need for enhanced and more coordinated national MCM surveillance during public health emergencies. The overarching goal of the IPT is to establish a comprehensive, PHEMCE-wide coordinated capability to collect, analyze, and enable assessment, decision-making, and communication of information about MCM use necessary to support an informed and efficient public health response during emergencies and for future responses. The IPT is currently focused on four core capabilities for MCM surveillance: collecting data on MCM use; managing, analyzing, and interpreting data on MCM use; incorporating key evidence into recommendations on MCM use; and communicating evidence-based recommendations. The IPT includes federal members who have reach back to state and local public health agencies to ensure coordination across all levels of public health.

The FDA AE-MAP was a one-year project to assess the feasibility of leveraging existing electronic health record (EHR) systems, from both inpatient and outpatient settings, to conduct near real-time monitoring and assessment of adverse events and relevant health outcomes associated with MCMs used during public health emergencies. Using seasonal influenza as a proxy, AE-MAP developed a data mining strategy and analytical approaches to identify potential adverse events and relevant health signals of interest. AE-MAP also identified specific data elements that provide meaningful information about MCMs used to diagnose, prevent, and treat influenza and pneumonia, and assessed whether these types of activities can be achieved in near real-time.[20]

MCM surveillance is also an area of focus within Mini-Sentinel. Through Mini-Sentinel there is an opportunity to expand current safety surveillance capabilities for MCMs and support a more comprehensive and timely approach to MCM safety surveillance. The sections below discuss a process for using Mini-Sentinel to conduct safety surveillance for MCMs dispensed outside of the traditional healthcare delivery system via PODs. The key components to this process include (1) electronically capturing individual-level MCM exposure data, (2) linking individuals' MCM exposure data to their electronic healthcare data for those individuals with electronic healthcare data available through a Mini-Sentinel Data Partner, and (3) subsequently matching this linkage to the Data Partners' local Mini-Sentinel data system, which will allow for Mini-Sentinel-initiated queries of health outcomes among individuals exposed to the MCM(s) of interest.

A. CAPTURING MCM EXPOSURE DATA ELECTRONICALLY

The primary purpose of a POD is to quickly dispense preventive medication to large numbers of people during a public health emergency. While POD plans include data collection activities, they have not focused on processes or capacities for electronic data collection, nor on subsequent planning for linkage of MCM exposure data to electronic healthcare data. However, this is changing as our healthcare and public health systems and functions adapt to the demand for greater availability and use of electronic healthcare data.

Given the conditions and requirements of MCM dispensing at PODs, methods and tools that utilize mobile technology to electronically capture data will likely be most effective. Mobile technology lends itself to supporting the various POD environments and is an efficient method for accurately capturing data. One example of a mobile application and device for collecting data is Denver Public Health's (DPH's) Hand-held Automated Notification for Drugs and Immunizations (HANDI) application. DPH developed HANDI to support efficient public health immunization and prophylaxis activities through the rapid collection and transfer of standardized electronic data. HANDI includes the mobile app and a server-based administration tool and relational database. HANDI operates on commonly available mobile devices (e.g., iPhone, iPod touch) that have photographic capability and are equipped with a magnetic stripe reader and barcode scanner. HANDI uses these tools and technologies to capture standardized patient data available through magnetic stripes or 2-D barcodes, such as those on driver's licenses and health insurance identification cards, as well as to capture photographic images of the data, if necessary. Data can also be entered manually using standard keyboard functions.

Information specific to the public health event is pre-incorporated into the data collection process using HANDIMan, the HANDI administration tool and event manager. Prior to an event, the intervention is defined by parameters including vaccine lot number, manufacturer, etc. and eligibility and contraindication questions related to the intervention being delivered. Authorized device usernames and passwords are also established. Once the intervention is defined within HANDIMan, it is downloaded onto the mobile devices.

Data collected via HANDI is saved on the device and transferred to the HANDI server-based database. Data transfer can take place in three ways: (1) a HANDI-dedicated network where all application components communicate in real-time via a HANDI Wi-Fi access point; (2) a network where all components communicate via an existing network; and (3) a disconnected environment where data are securely stored on the devices until a connection to the HANDI server is established. The HANDI server bundles the collected data into a patient record, which can be transferred to a designated database (e.g., EHR) or registry (e.g., state immunization registry). The HANDIMan administration tool provides the capability to export the data using Health Level Seven (HL7) messaging, as well as via relational and flat file formats.

Both the mobile device and the HANDI application are password protected, the data is encrypted using Advanced Encryption Standard (AES) 256, and data are transferred using secure network environments.

Additionally, mobile device management software is installed so that the device can be "wiped" if it is lost or stolen.

DPH has successfully used HANDI during vaccination campaigns, including Denver Health's annual employee influenza campaign and childcare worker pertussis vaccination outreach. Additionally, through Mini-Sentinel's MCM surveillance activities, DPH, in collaboration with Kaiser Permanente Colorado (KPCO, a Mini-Sentinel Data Partner), FDA, and the National Association of County and City Health Officials (NACCHO), conducted a field test using HANDI to provide a proof-of-concept for incorporating data collected outside of a Mini-Sentinel Data Partner system into the local Data Partner Mini-Sentinel Distributed Database (MSDD). The results of the field test indicate that HANDI technology could be utilized to support data collection and linkage during a public health emergency. See Section IV for a summary of the field test.

Data collected at PODs must include individual MCM exposure and MCM event information to facilitate the process of linking the MCM exposure data to electronic healthcare data, and to provide data elements for matching individuals represented in multiple data systems. The data fields listed below represent the fields likely to be necessary for this to occur.

Individual Identifying Data Fields

- First and last name
- Date of birth
- Gender
- Health insurance provider(s) and member identification number(s)

Additional elements (e.g., address, phone number, e-mail address, and driver's license number) may improve the rate of matching or facilitate follow-up, if necessary, but are not essential for a basic match.

Current data collection practices at PODs do not include the collection of health insurance information, since MCM costs are not billed to recipients. The proposed process for use of Mini-Sentinel to support improved MCM safety surveillance requires the collection of health insurance information to enable linkage to electronic healthcare data. Under the proposed process, health insurance information is not collected for any reason other than to facilitate linkage to electronic healthcare data contained within the Data Partners' systems. Challenges and limitations to the collection and use of health insurance information for MCM safety surveillance include: some individuals do not have health insurance, some individuals may be reluctant or refuse to provide their health insurance information (this may also be true for driver's license information), and some health insurance providers, including non-commercial providers, are not Data Partners. Health departments and their public health preparedness partners can mitigate the impact of these challenges and limitations through public education efforts about why this information is being collected.

MCM and Public Health Event Data Fields

- National Drug Code (NDC)
- Dosage
- Manufacturer
- Lot number
- POD site
- Date and time

Ideally these fields will be pre-populated through the event manager system. Medical product information may also be obtained by scanning the 2-D barcode for the medical product, if provided.

The benefits of capturing data using mobile and scanning technology include reductions in collection time, response burden, and errors resulting from manual entry, as well as adaptability to the variety of methods and settings for MCM dispensing. Additionally, the capability to transfer data in real- or near real-time to a specified data repository or entity, such as a Mini-Sentinel Data Partner, greatly enhances the opportunities for timely use of the data. However, the majority of jurisdictions across the country do not currently use or have access to mobile, or even electronic, data collection technology, which presents challenges that will need to be addressed in order for the process proposed in this report to be implemented.

Data sources also present challenges to the process. There is currently no national standard for how information is formatted and stored on health insurance cards and driver's licenses. Some cards are equipped with magnetic stripes, others with barcodes, and others only have visible information, which may be stored in different places. Additionally, for those cards with a magnetic stripe or barcode, how the information is coded varies. To collect the desired data fields, information on how data is formatted and stored needs to be known ahead of time so that the technology can be programmed to identify, read, and collect the desired information. Alternative strategies to data collection, such as Web-based pre-event registration, could be utilized to mitigate challenges related to inconsistencies in data formatting. Such strategies would also help address the challenge presented by individuals who do not present to the POD with their personal identification and health insurance cards (e.g., health insurance card left at home).

Challenges to electronically capturing the desired data may also arise based on how the POD is structured. For example, the ability to capture data on every individual exposed to the MCM is limited for delivery methods that do not require every individual to visit a POD. It must also be recognized that dispensing data does not necessarily mean exposure data; however, in cases where exposure cannot be guaranteed, data that the MCM was dispensed is the best proxy available.

A final challenge to note is that some individuals may be reticent or object to providing the requested information due to concerns about privacy and confidentiality. Despite these challenges, technologies and systems for electronic and mobile data collection are continuously being explored, updated, refined, and advanced. As tools and systems become more sophisticated and routinized, the number of challenges to electronic data capture, as well as linkage, will be reduced. Furthermore, the field test conducted by DPH and KPCO demonstrated the feasibility of using a mobile device to collect patient information and accurately link individuals to their electronic health record.

B. LINKING AND MATCHING MCM EXPOSURE DATA TO HEALTH OUTCOMES DATA

Linking and matching MCM exposure data to health outcomes data, and subsequently to Data Partners' MSDD, is a multi-step process that will require coordination and cooperation among multiple agencies, organizations, and systems. The key steps in this process include sharing electronic, individual-level MCM exposure data with the appropriate Data Partners; matching exposure records to individual patient records within the Data Partners' information systems; and linking matches to the Data Partners' MSDD, which will allow for exposure-outcome assessments.

1. Sharing MCM Exposure Data

During a public health emergency, MCM dispensing is likely to occur at multiple locations by multiple public health agencies and healthcare organizations, potentially across multiple jurisdictions and states. The data collected at PODs during the course of an MCM event is managed by the public health system. The public health system will need to coordinate with its healthcare partners to organize and securely store electronic MCM exposure data and to support electronic transfer of individual level MCM exposure data from the public health system to the correct Mini-Sentinel Data Partner. Discussion of public health's organization and storage of electronic MCM exposure data is outside the scope of this report; however, it is a critical component in the process and must be explored further.

Each Data Partner should only receive or have access to MCM exposure data for the patients represented in its system, so the data collected by public health at PODs will need to be organized by Data Partner. This could be accomplished by applying a simple SQL query at the point of MCM exposure data coordination/storage (e.g., server-based database). The query would utilize the collected health insurance provider information to identify and organize the data by Data Partner. Once the MCM exposure data is organized as such, it can then be shared with the Data Partners.

Ongoing Mini-Sentinel efforts exploring data exchange, linkage, and systems interoperability shed light on methods for securely, successfully, and rapidly sharing data between data systems outside of Mini-Sentinel and its Data Partners. For example, the PRISM team is working to develop interoperability specification to standardize data exchange between PRISM Data Partners and immunization registries.[21] This work reinforces the benefit of adopting HL7 specification, a key factor that supports the two-way exchange of information. Adoption of HL7 is a key component of Meaningful Use.[22] As compliance with Meaningful Use standards expands, the infrastructure for the meaningful use of interoperable electronic healthcare data will further support the type of data exchange and use proposed here.

The most feasible methods for getting MCM exposure data to the Data Partners will likely involve "pushing" it to them. Options for this include exchanging data by sending it in batches or preferably by using a transport layer to exchange data automatically. Transport layer technologies provide the infrastructure to transfer HL7 messages from the HL7 sender to the HL7 receiver. Without automated transfer technology, data must be exchanged in batches, which requires manual intervention. There may also be limitations on batch size, requiring multiple batches to be sent. During a public health emergency, automated transfer of MCM exposure data would allow for more efficient transfer and timely use of the data; however, transport layer software can be costly, which may be prohibitive for many public health systems.[23] Efforts are underway to develop lower-cost transport layer technology, which have the potential to go a long way to support MCM safety surveillance activities, as well as other data exchange activities. Though transport layer technology will come at a financial cost, automated data transfer removes the need for manual intervention to exchange batches of data, which also comes at a cost.

Alternatively, processes by which Data Partners "pull" data from public health for their patient population involved in the MCM event could be utilized. However, these methods are likely to be more complicated from both procedural and security standpoints and are not currently suggested over "push" mechanisms.

Implementation of statewide health information exchanges (HIEs) offers another, and potentially the most preferential, approach for sharing MCM exposure data with the Data Partners. HIEs have the potential to provide a single point of contact for all public health data within a state or jurisdiction. As HIE implementation expands across the country, this approach should be explored further.

2. Matching MCM Exposure Data to Patient Data/Records

Once the Data Partner receives their subset of the MCM exposure data, or gains access to the data via another mechanism, they will need to match it to the corresponding patient data/records within their information systems. This process is likely to occur using matching algorithms that employ the individually information collected at PODs. It should be recognized that the sensitivity and specificity of matching algorithms will have implications for the interpretation and use of the results. Possible outcomes from matching include: true positive (a match with the correct person); false positive (a match, but with the incorrect person); true negative (no match, but the person is not currently represented in the Data Partners information); and false negative (no match, but the person is currently represented in the Data Partners information). Understanding the implications of these possibilities is essential, as this step identifies the population of interest for assessment of health outcomes associated with receipt of the MCM (i.e., it establishes the denominator).

Use of HL7 would also greatly facilitate the matching process; however, until HL7 is universally implemented, data matching processes and algorithms will need to take into consideration interoperability specifications, including data standardization, which will influence the efficiency and success of the matching process. Data standardization includes issues such as the use of hyphens and abbreviations (e.g., Road, Rd., RD) and differences in name order (e.g., first/middle/last, last/first/middle). Using programs to standardize data fields before matching could facilitate the process and increase the match rate; however the cost of these programs and the time to run them present challenges to their use, especially during a public health emergency.

3. Linking Matches to Data Partners’ Local Mini-Sentinel Distributed Database

Once matches between MCM exposure data and the Data Partners’ patient information systems are made, a matched dataset will be established, which must then be linked to the Data Partner’s local MSDD. This step in the process is what ultimately enables the externally collected MCM exposure data to be incorporated into the MSDD, and thus available for query. This linkage may be performed using a cross-walk from the “MCM dataset” to the Mini-Sentinel CDM) which is a data structure that standardizes administrative and clinical information across Data Partners. Transforming data into the CDM makes it possible to execute queries developed by MSOC.

The ability to incorporate externally collected data into Mini-Sentinel has been demonstrated through the PRISM project, as well as through the Mini-Sentinel Medical Countermeasure Surveillance Field Test described in Section IV. Through PRISM activities, immunization registries send immunization data to Data Partners and the Data Partners convert the data into the Mini-Sentinel CDM standard State Vaccine file format.[24] For the purpose of MCM safety surveillance, it will need to be determined how the dispensed drugs and vaccines are identified as MCMs within the CDM or how modular programs can be developed to recognize exposure to a particular drug or vaccine as a MCM, as opposed to exposure to the medicine for reasons unrelated to the public health event.

Conducting and managing data matching and linkage are not without challenges, many of which have already been discussed. Challenges include interoperability, data transfer technology, infrastructure for secure information exchange, data sharing rules and regulations, and resource limitations. The unique circumstances associated with MCM dispensing and safety surveillance during public health emergencies exacerbates these challenges, in particular timeliness and resource requirements. New methods, technologies, and tools may need to be developed to specifically support MCM safety surveillance capabilities. However, continued work to refine and improve capabilities that support non-emergency or routine safety surveillance and data exchange will support expanded use (i.e., surge capacity) during emergency events.

C. CONDUCTING EXPOSURE-OUTCOME ASSESSMENTS

Once the MCM exposure data is incorporated into the MSDD, the Mini-Sentinel standardized programs designed to query the database can be programmed to identify individuals who were exposed to the MCM and also experienced the health outcome(s) of interest. Query results can be analyzed locally and aggregated data is returned to the MSOC for evaluation.

A significant number of Mini-Sentinel efforts have focused on developing and refining techniques for identifying, validating, and linking medical product exposures and health outcomes. Numerous projects have also focused on determining which codes in EHR data and administrative claims-based data are the most valid and reliable indicators of the presence of particular medical conditions. From a procedural standpoint, these methods do not need to be altered to conduct MCM safety surveillance.

However, the ability to use administrative claims-based data to rapidly identify health outcomes is limited by the amount of time it takes for the information to enter into the claims system and stabilize, as well as the length of time for it to be available for query through Mini-Sentinel. Most Mini-Sentinel data are currently refreshed on a quarterly basis and contain relatively settled and complete data, the most recent of which are on average 6-9 months old. Near real-time surveillance will require more frequent data updates and fresher data in datasets.

The Mini-Sentinel PRISM Sequential Analysis Workgroup is working on these issues. Specifically, they are (1) evaluating the usefulness of conducting surveillance with fresher data that is more timely but incomplete and requires more effort to utilize and (2) developing new methods to use freshest feasible data.[25] Through these activities, Katherine Yih and colleagues have demonstrated that it is feasible to access, conduct quality control measures, and analyze Mini-Sentinel data on exposures and health outcomes occurring as recently as six weeks in the past (i.e., six weeks from last care-date in the data to results of sequential analysis).[26] As these capabilities are further developed and refined, the opportunity for Mini-Sentinel to support improved MCM safety surveillance during and immediately following public health emergencies will be increased.

Administrative claims-based data does not include care paid for out-of-pocket or events which are not associated with a healthcare encounter that is billed for, such as deaths. Additionally, since Data Partners are predominantly commercial providers, some populations (e.g., Medicare, Medicaid, and the Veterans Health Administration) are not well represented in the Mini-Sentinel data. While these challenge does not preclude the use of this data or minimize its value for safety surveillance, they must be taken into consideration when analyzing and interpreting the data. The use of complementary data sources, such as immunization registries, disease registries, and HIEs, may help address this potential gap in data by increasing the data available to Mini-Sentinel. Additionally, Mini-Sentinel is currently assessing the potential for linkage with the National Death Index+ to ascertain causes of out-of-hospital deaths. Timeliness and data accessibility and interoperability similarly pose challenges to the efficient use of complementary data sources during public health emergencies. However, continued focus on efforts to expand data availability, interoperability, and meaningful use will benefit MCM safety surveillance, as well as safety surveillance overall.

IV. MINI-SENTINEL MEDICAL COUNTERMEASURE SURVEILLANCE FIELD TEST

Through Mini-Sentinel's MCM activities, the Mini-Sentinel Medical Countermeasure Surveillance Field Test was conducted to serve as a proof-of-concept for the key steps in the process proposed in the previous section.[27] The goal of the field test was to determine whether patients presenting for care at a primary care clinic within the KPCO (a Mini-Sentinel Data Partner) healthcare system could be uniquely identified using an external mobile data collection system, accurately matched to their individual medical record within KPCO, and subsequently linked to the local KPCO Mini-Sentinel database. The broader purpose of the field test was to develop capacity to assess safety outcomes of exposures to drugs and vaccines administered as MCMs, especially in non-traditional healthcare settings (e.g., PODs), in response to a public health emergency.

The project team was comprised of representatives from Mini-Sentinel, FDA, DPH, KPCO, and NACCHO. A protocol was developed to match externally collected MCM data for KPCO members to KPCO's information systems and link to the local KPCO MSDD. The team conducted the field test from November 2013 through January 2014 at KPCO routine patient registration and at an influenza immunization clinic at a single primary care facility within the KPCO system.

DPH's HANDI mobile data collection tool was used to capture the externally collected information (standardized, encrypted patient demographic and vaccination information). When patients presented for care, the HANDI device was used to scan the patient's driver's license, photograph their KPCO member ID card (considered the "gold standard" of true patient identity within the KPCO system), manually enter their KPCO member ID, and capture influenza vaccination information.

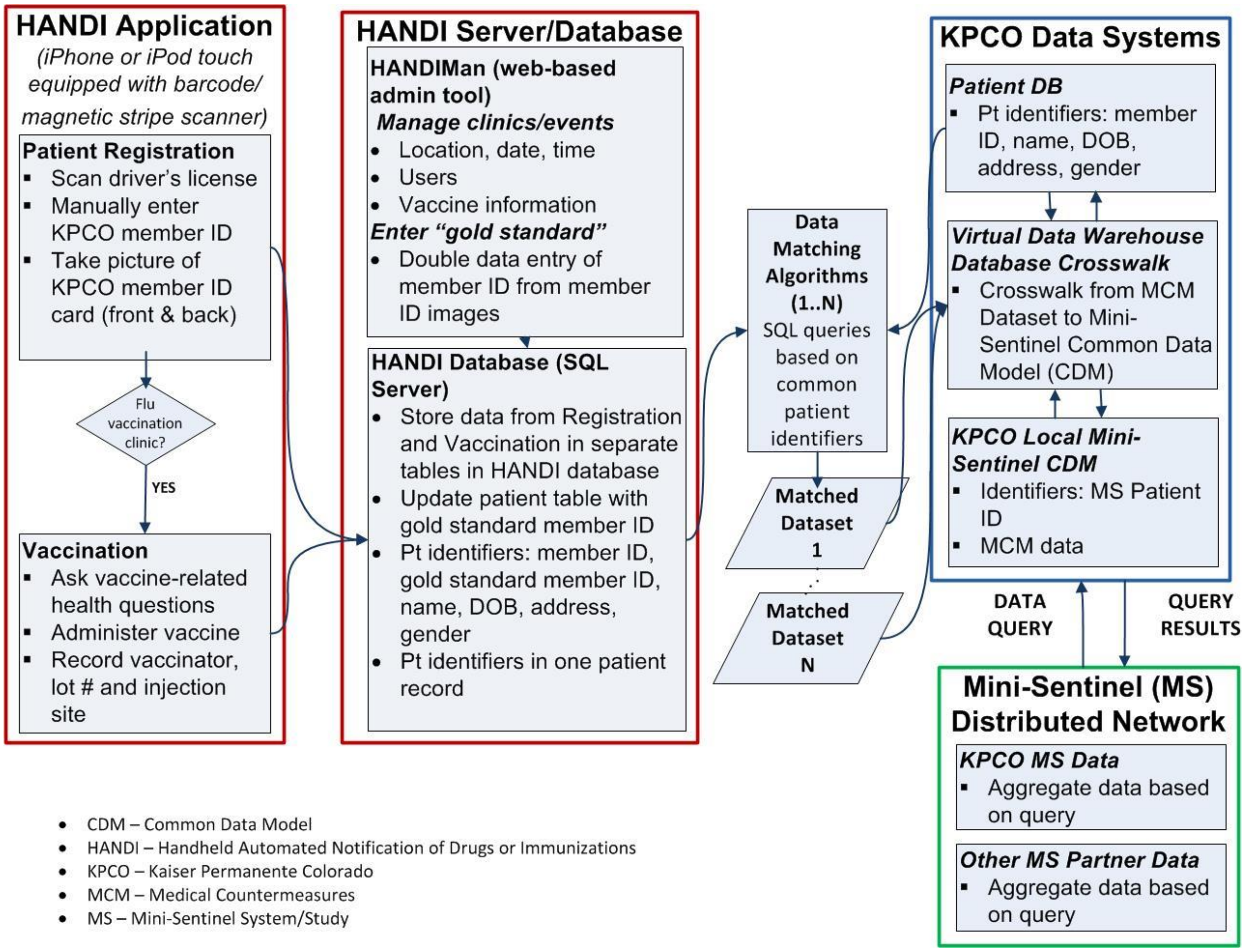
For the patient registration component, a total of 464 individuals were approached while checking in for routine care; of these, 431 (93%) agreed to participate, and 33 (7%) declined participation. Among the 431 who agreed to participate, 10 subjects did not have a readable photograph of their KPCO health insurance card, and therefore did not have a "gold standard" of their true identity. These 10 subjects were excluded from all analyses. All 421 subjects included in analyses had a first name, last name, and plausible date of birth extracted from their driver's license.

Algorithms were applied to match the HANDI collected data to KPCO electronic health records and then link to the local KPCO MSDD. When using the exact last name, first name, and date of birth from the driver's license, 382 of 421 (91%) were matched with a patient from the KPCO enrollment database, while 39 of 421 (9%) were not matched. Among the 382 individuals with a match, the health record for 5 individuals (1%) did not match the health record number (HRN) from the gold standard. Among the 377 individuals with a match of HRN to the gold standard, 374 (99%) were matched to the Mini-Sentinel CDM used for surveillance. Taking these matching steps in aggregate, among the 421 individuals participating in the field test, 374 (89%) were correctly matched and linked to a record within Mini-Sentinel.

The HANDI device was also piloted during the annual fall influenza vaccination campaign at KPCO to determine whether the device could accurately collect detailed information about influenza vaccines administered to KPCO members. In addition to the driver's license and KPCO member ID card information, the following vaccination-related data points were also collected: specific antigen (e.g., influenza), lot number, manufacturer, expiration date, dose, site (e.g., right deltoid), administrator, and administration date. A total of 21 individuals participated in this part of the pilot. Of these 21 participants, all were accurately matched to the "gold standard" HRN. Among the vaccination-related data elements, only vaccination site (i.e., right deltoid versus left deltoid) was not matched with 100% accuracy.

Figure 1 shows how KPCO member data was collected and linked during the field test. Data was collected using HANDI and transferred to the HANDI server. Matching algorithms were applied to the HANDI and KPCO data systems to produce the matched datasets which were then linked to the KPCO MSDD. Once incorporated into the KCPO MSDD, the data could be queried as part of the MSDD by a modular program written by MSOC and distributed to Data Partners. This data flow is analogous to the data flow described in Section III.

Figure 1. Field test data flow


HANDI Application
(iPhone or iPod touch equipped with barcode/ magnetic stripe scanner)
Patient Registration
▪ Scan driver's license
▪ Manually enter KPCO member ID
▪ Take picture of KPCO member ID card (front & back)
Flu vaccination clinic?
YES
Vaccination
▪ Ask vaccine-related health questions
▪ Administer vaccine
▪ Record vaccinator, lot # and injection site
HANDI Server/Database
HANDIMan (web-based admin tool)
Manage clinics/events
• Location, date, time
• Users
• Vaccine information
Enter "gold standard"
• Double data entry of member ID from member ID images
HANDI Database (SQL Server)
• Store data from Registration and Vaccination in separate tables in HANDI database
• Update patient table with gold standard member ID
• Pt identifiers: member ID, gold standard member ID, name, DOB, address, gender
• Pt identifiers in one patient record
Data Matching Algorithms (1..N)
SQL queries based on common patient identifiers
Matched Dataset 1
Matched Dataset N
KPCO Data Systems
Patient DB
▪ Pt identifiers: member ID, name, DOB, address, gender
Virtual Data Warehouse Database Crosswalk
▪ Crosswalk from MCM Dataset to Mini-Sentinel Common Data Model (CDM)
KPCO Local Mini-Sentinel CDM
▪ Identifiers: MS Patient ID
▪ MCM data
DATA QUERY
QUERY RESULTS
Mini-Sentinel (MS) Distributed Network
KPCO MS Data
▪ Aggregate data based on query
Other MS Partner Data
▪ Aggregate data based on query

- CDM – Common Data Model
- HANDI – Handheld Automated Notification of Drugs or Immunizations
- KPCO – Kaiser Permanente Colorado
- MCM – Medical Countermeasures
- MS – Mini-Sentinel System/Study

The field test demonstrated the feasibility of using a mobile device to collect patient information and accurately match individuals to their electronic health record within the KPCO system, and link to KPCO's local MSDD. It also demonstrated that HANDI is capable of capturing detailed and accurate information about administration of influenza vaccine, a capacity that is analogous to what may be needed to capture information about a MCM during a public health emergency. The results of the field test are supportive of the processes proposed in this report. Limitations of the field test include: it was not conducted in the context of a true MCM event and it was only conducted among KPCO members, as opposed to the general population. KPCO members presenting for care at KPCO may be more likely to participate in sharing their driver's license information than the public would be to share this information in a true MCM event; and while the KPCO population is generally representative of the population of Colorado, these results may not generalize to specific populations, such as the uninsured.

In a true MCM event, multiple MCM exposure data sources and Data Partners are likely to be involved, requiring sophisticated methods and plans for data query and capabilities to either "push" or "pull" data from the MCM event to the correct healthcare organization for each individual. Further field testing will need to assess these methods and to refine existing and develop new methods, tools, and technologies to support the unique circumstances encountered during an MCM event.

V. PRIVACY AND CONFIDENTIALITY CONSIDERATIONS (BY KRISTEN ROSATI)

This section addresses privacy and other legal issues involved in utilizing Mini-Sentinel to improve safety surveillance for MCMs dispensed via PODs through the process detailed in Section III, components of which were piloted in the field test summarized in Section IV.[28] The following discussion addresses compliance with the Health Insurance Portability and Accountability Act and its regulations (HIPAA), concluding that most PODs will not be covered by HIPAA. This section also addresses the application of state laws, and notes that PODs should examine any state law applicable to them to confirm that the use of identifiable health information for public health surveillance is permitted. Next, this section discusses whether MCM safety surveillance activities are "research" requiring review by an Institutional Review Board (IRB), concluding that these activities are public health practice, not research.

A. COMPLIANCE WITH HIPAA

HIPAA likely will not apply to the great majority of PODs, such as public health agencies, schools, private businesses, and the like. HIPAA applies only to "covered entities" and their "business associates."[29] Covered entities are health plans, healthcare clearinghouses, and healthcare providers that engage in "standard transactions" (typical financial and business transactions with health plans).[30] Business associates are persons or entities that receive protected health information (PHI) in order to provide services to covered entities.[31] Only a limited number of PODs will be HIPAA covered entities, such as physician clinics, long term care facilities, and other facilities in the traditional health care system. Most PODs will not be HIPAA covered entities or business associates, such as public health and other government agencies, public schools, and employers.

Some PODs will be HIPAA "hybrid entities"—organizations that have carved out the functions within their organizations that must comply with HIPAA (called "health care components"), so that HIPAA does not apply to the entire organization.[32] For example, many universities have created hybrid entities, under which their student health services or other provider functions fall within the HIPAA covered entity as health care components. In that case, HIPAA would not apply to the university as a whole, but would cover only the activities of the health care components. Whether HIPAA would apply to a POD activity at a HIPAA hybrid entity would depend on where that POD activity was "housed" and which personnel provide the POD-related activities.

HIPAA also does not affect covered entities' employee health functions. Health information collected in an organization's role as an employer is not PHI, and thus is not protected by HIPAA.[33] For example, if a hospital conducts a POD activity for its employees as part of its employee health program, that activity would not generate PHI that is protected by HIPAA. Of course, if a hospital or other covered entity administers the MCM to its patients (not just its employees), then that POD activity is conducted in its role as a healthcare provider (which is covered by HIPAA).

Finally, HIPAA would not apply to the activities of a POD's employees at a HIPAA covered entity location. For example, if a local health department conducts POD activities in the lobby of a local hospital, that activity will not be covered by HIPAA unless on-duty hospital personnel assist in the effort. That is because any health information collected by the health department would not be created or received by the covered entity.[34]

Each organization that has HIPAA covered entity functions should evaluate how the law applies to its particular POD activity. Appendix A addresses the HIPAA compliance obligations of PODs that are HIPAA covered entities or business associates. It concludes that HIPAA permits disclosure of identifiable health information for MCM surveillance without individual permission, because MCM activities fall within a broad HIPAA exception for public health activities.

B. COMPLIANCE WITH STATE LAW

Entities that collect and disclose individually identifiable information for MCM delivery/administration and safety surveillance should confirm that they are doing so in compliance with any applicable state health information confidentiality laws. There are a wide variety of state laws that regulate health information confidentiality, including laws that regulate certain types of information (e.g., information about communicable disease, HIV, genetic testing, mental health and substance abuse, disability), and laws that regulate certain types of licensed entities (e.g., hospitals, nursing homes, clinics, physician offices). It is very common for these laws expressly to permit disclosure of identifiable health information for public health functions, but each POD should confirm that their planned disclosures in the context of MCM safety surveillance activities comply with any state laws applicable to it.

C. INSTITUTIONAL REVIEW BOARD REVIEW

The activities described in this report are not "research" that requires IRB review. The distinction between "public health practice" and "public health research" is often a thin one, and has been widely discussed in the academic and public health literature.[35] CDC explained the problem with distinguishing between public health practice and research:

> The regulations state that "research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." [45 C.F.R. § 46.102] Obtaining and analyzing data are essential to the usual practice of public health. For many public health activities, data are systematically collected and analyzed, blurring the distinction between research and non-research. Scientific methodology is used both in non-research and research activities that comprise the practice of public health. Because scientific principles and methodology are applied to both non-research and research activities, knowledge is generated in both cases. Furthermore, at times the extent to which that knowledge is generalizable may not differ greatly in research and non-research. Thus, non-research and research activities cannot be easily defined by the methods they employ. Three public health activities - surveillance, emergency responses, and evaluation - are particularly susceptible to the quandary over whether the activity is research or non-research.[36]

As the methodology used in public health activities become increasingly sophisticated and systematic, and the principals of those activities choose to publish their results to benefit the larger community, the distinction between public health activities and research will be increasingly unworkable.[37]

However, despite the uncertainty about what constitutes public health practice versus research, the MCM safety surveillance activities described in this report clearly fall on the side of public health *practice*. As the CDC explains: “Most emergency responses tend to be non-research because these projects are undertaken to identify, characterize, and solve an immediate health problem and the knowledge gained will directly benefit those participants involved in the investigation or their communities.”[38]

Moreover, the MCM safety surveillance activities conducted by the Data Partners, MSOC, and FDA are not research. The HHS Office for Human Research Protections (OHRP) has concluded that activities related to the Sentinel Initiative are <u>not</u> covered by 45 C.F.R. Part 46 (“the Common Rule”). This means that Sentinel Initiative activities are not research that requires review by an IRB. On January 19, 2010, Jerry Menikoff, Director of the OHRP, wrote a letter to Rachel Behrman, Acting Associate Director of Medical Policy, Center for Drug Evaluation and Research at the FDA, explaining that OHRP “has determined that the regulations this office administers (46 CFR part 46) do not apply to the activities that are included in the [FDA] Sentinel Initiative.”[39] Dr. Behrman then wrote on April 2, 2010, to Dr. Richard Platt at Harvard Pilgrim Health Care (the Mini-Sentinel’s prime contractor managing the Coordinating Center), providing Dr. Menikoff’s letter and concluding that the OHRP’s “assessment applies to the work being conducted by [Harvard Pilgrim Health Care] and its subcontractors under contract number HHSF2232009100061, as the purpose of this contract is to carry out Sentinel Initiative activities that are included in the [FDA] Sentinel Initiative.”[40] The activities within the MCM safety surveillance project are included within this referenced contract from FDA to the Coordinating Center. This means that data sources providing information for Mini-Sentinel purposes, including MCM safety surveillance activities, are not required by federal regulation to obtain approval of their IRBs for participation in Mini-Sentinel, and are not required to obtain a determination from their IRBs that these activities are “exempt.”

VI. CONCLUSION

The capacity to monitor the safety of MCMs during and after a public health emergency is of substantial public health importance. Though an extensive and growing framework for medical product safety surveillance exists, the discussions above highlight that a more robust, comprehensive, and timely approach to monitoring and assessing the safety of MCMs is needed. The Mini-Sentinel Medical Countermeasure Surveillance Field Test provides a proof-of-concept for the feasibility of improving MCM safety surveillance using Mini-Sentinel capabilities. Ongoing and future efforts will need to address current challenges to implementing the proposed process on a larger scale. The challenges primarily fall into two categories – technical and systems/infrastructure.

From the technical standpoint, the key challenges and areas for additional work include: electronic data collection and security, data formatting, data transfer, data linkage, and other technologies and tools to accommodate timely electronic capture, storage, transfer, and linkage. Data lag issues present technical, as well as analytical, challenges. Data lag exists both for MCM exposure data collected via PODs to get from health departments to the Data Partners, as well as for electronic healthcare data to enter data systems, stabilize, and become available. The MCM exposure data lag is likely to be significantly shorter than that for electronic healthcare data. As previously noted, Mini-Sentinel is actively engaged in efforts to increase access to the freshest feasible data for conducting safety surveillance; however, using fresher data presents analytical challenges, such as adjusting for data lag or for partial data (as opposed to mature data). This is also being explored through Mini-Sentinel activities and should be specifically explored within the context of MCM safety surveillance during and immediately following public health emergencies.

Systems-level challenges include: procedural changes to MCM dispensing data collection plans and capabilities; the majority of local health departments across the country are not equipped or resourced to support electronic data capture and EHRs; and current gaps and deficiencies in our health IT infrastructure. Continued movement towards implementation of HIEs, Meaningful Use, and standard formatting of electronic healthcare and public health data (i.e., HL7) will go a long way towards addressing these challenges by making the systems for public health and healthcare data sharing more fluid and established. Nevertheless, the basic requirements and procedures for improved MCM safety surveillance using Mini-Sentinel capabilities and data currently exist.

Achieving a more robust system for MCM safety surveillance will require coordination and collaboration across all levels of government and among multiple agencies, as well as with nongovernmental partners. Additional resources, including funding, guidance, training, and support, will also be needed, as well as oversight and authority to ensure appropriate implementation, data analysis and interpretation, and information dissemination to public health officials, clinicians, other decision makers, and the public. As evidenced by this and other federal efforts to strengthen and coordinate MCM surveillance capabilities, as well as efforts undertaken at the state and local levels, there is great momentum for this work and already demonstrated success. This report and the Mini-Sentinel Medical Countermeasure Surveillance Field Test provide essential information for moving forward with these efforts and should serve as a roadmap to guide future efforts.

VII. APPENDICES

A. APPENDIX A

Compliance with HIPAA

Section VI of the white paper on “HIPAA and Common Rule Compliance in the Mini-Sentinel Pilot”[41] discusses when HIPAA applies to MCM surveillance activities. This Appendix A discusses HIPAA compliance in MCM surveillance activities, for those organizations that are HIPAA covered entities or business associates.

1. If HIPAA Applies, Disclosures of PHI in Support of MCM Surveillance Are Permitted without Individual Authorization as a Public Health Activity

For those PODs that do have to comply with HIPAA, HIPAA permits disclosure of identifiable health information for MCM surveillance without individual permission, because MCM activities fall within a broad HIPAA exception for public health activities.

HIPAA has a broad exception that permits HIPAA covered entities to disclose PHI without the authorization of individuals[42] for a variety of public health activities.[43] These include disclosures of PHI to:

> A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.[44]

Assessment of health outcomes after administration of an MCM clearly is for the “conduct of public health surveillance.” MCM safety surveillance is consistent with the FDA’s mission to protect and promote the public health through the Sentinel Initiative.[45]

Moreover, state or local public health agencies are public health authorities, as is any third party under contract with those agencies.[46] For purposes of Mini-Sentinel activities, such as MCM safety surveillance, the MSOC and the Data Partners are “public health authorities” under HIPAA, as they are “acting under a grant of authority from or contract with” the FDA. The FDA has a contract in placed with the MSOC, and the MSOC has subcontracts in place with the Data Partners. Even though the Data Partners do not have a direct contract with the FDA, FDA has issued a letter to the MSOC explaining that both MSOC and its subcontractors are acting under a grant of authority from the FDA.[47] Thus, PHI may flow from PODs that are HIPAA covered entities or business associates to the MSOC and to the Data Partners as “public health authorities” for the purpose of MCM safety surveillance within the Mini-Sentinel system.

2. If HIPAA Applies, Verification of Identity and Authority to Request PHI Is Required

To disclose PHI to the FDA or an entity acting under a contract or other grant of authority from the FDA, PODs that are HIPAA covered entities must confirm the recipient’s identity and that the recipient has the legal authority to request the PHI.[48] A covered entity is entitled to rely on written confirmation on FDA letterhead that the MSOC and the Data Partners are acting on behalf of the FDA, and that they have the legal authority to request PHI for Mini-Sentinel purposes.[49] FDA has issued such a letter to the MSOC explaining that both the MSOC and the Data Partners are acting under a grant of authority from the FDA.[50] In other words, HIPAA covered entities are not expected to make their own independent inquiry into whether sending PHI to the FDA, the MSOC, or the Data Partners serves a legally authorized public health purpose.

PODs that are not HIPAA covered entities are not subject to this HIPAA verification requirement.

3. If HIPAA Applies, PODs Must Comply with the Minimum Necessary Standard

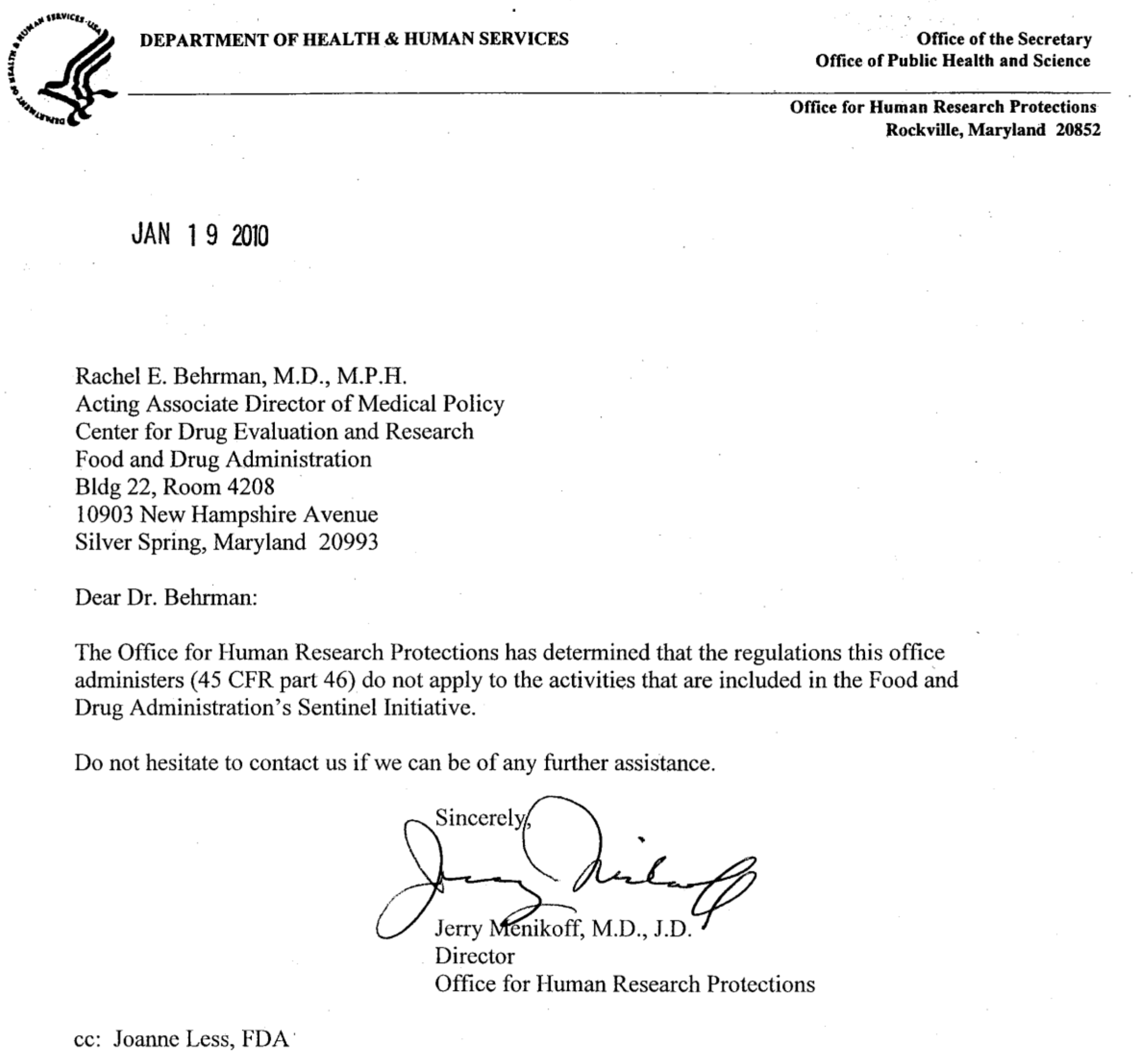
HIPAA covered entities must observe the “minimum necessary standard” in releasing PHI for public health purposes. This simply means that a covered entity must make reasonable efforts to limit the information to the minimum amount of information that is necessary to accomplish the intended purpose of the disclosure,[51] with some limited exceptions not relevant here.[52] A covered entity may not disclose the entire medical record unless there is a specific justification for doing so.[53]

Under the HIPAA Privacy Rule, a covered entity may rely on a public health authority’s determination that the data requested are the minimum necessary data that the agency needs to fulfill the purpose of its request.[54] If the FDA, the MSOC or Data Partners provide documentation that the information requested in the MCM surveillance is limited to that required to evaluate the MCM safety, covered entities may rely on that minimum necessary determination. In the absence of that documentation, PODs that are covered entities should document that determination themselves. Given the limited information collected in the MCM surveillance plan, that information likely would meet the minimum necessary standard.

PODs that are not HIPAA covered entities are not subject to the HIPAA minimum necessary standard.

B. APPENDIX B

1. Exhibit 1



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary
Office of Public Health and Science

Office for Human Research Protections
Rockville, Maryland 20852

JAN 19 2010

Rachel E. Behrman, M.D., M.P.H.
Acting Associate Director of Medical Policy
Center for Drug Evaluation and Research
Food and Drug Administration
Bldg 22, Room 4208
10903 New Hampshire Avenue
Silver Spring, Maryland 20993

Dear Dr. Behrman:

The Office for Human Research Protections has determined that the regulations this office administers (45 CFR part 46) do not apply to the activities that are included in the Food and Drug Administration's Sentinel Initiative.

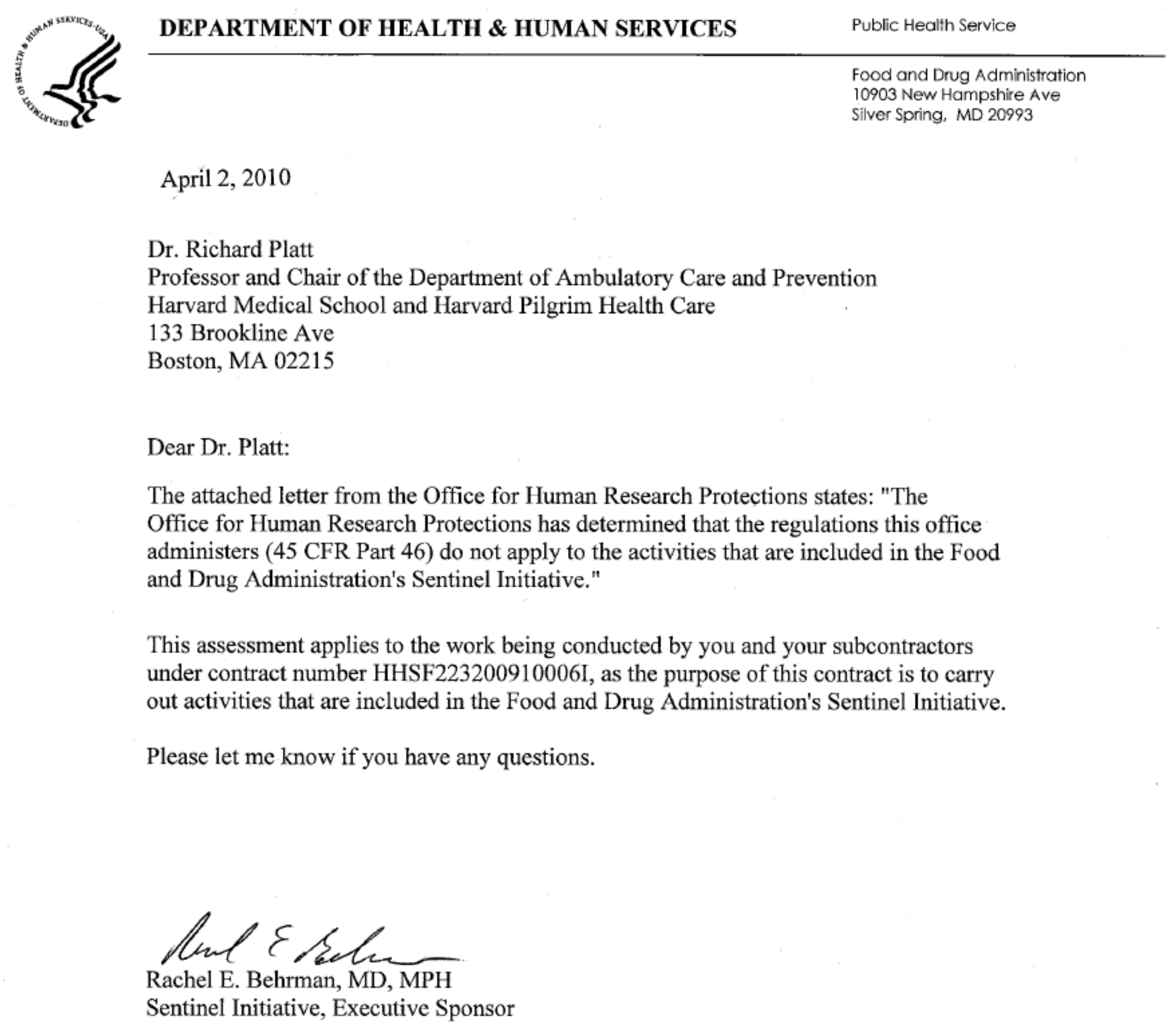
Do not hesitate to contact us if we can be of any further assistance.

Sincerely,

Jerry Menikoff, M.D., J.D.
Director
Office for Human Research Protections

cc: Joanne Less, FDA

2. Exhibit 2



DEPARTMENT OF HEALTH & HUMAN SERVICES Public Health Service

Food and Drug Administration
10903 New Hampshire Ave
Silver Spring, MD 20993

April 2, 2010

Dr. Richard Platt
Professor and Chair of the Department of Ambulatory Care and Prevention
Harvard Medical School and Harvard Pilgrim Health Care
133 Brookline Ave
Boston, MA 02215

Dear Dr. Platt:

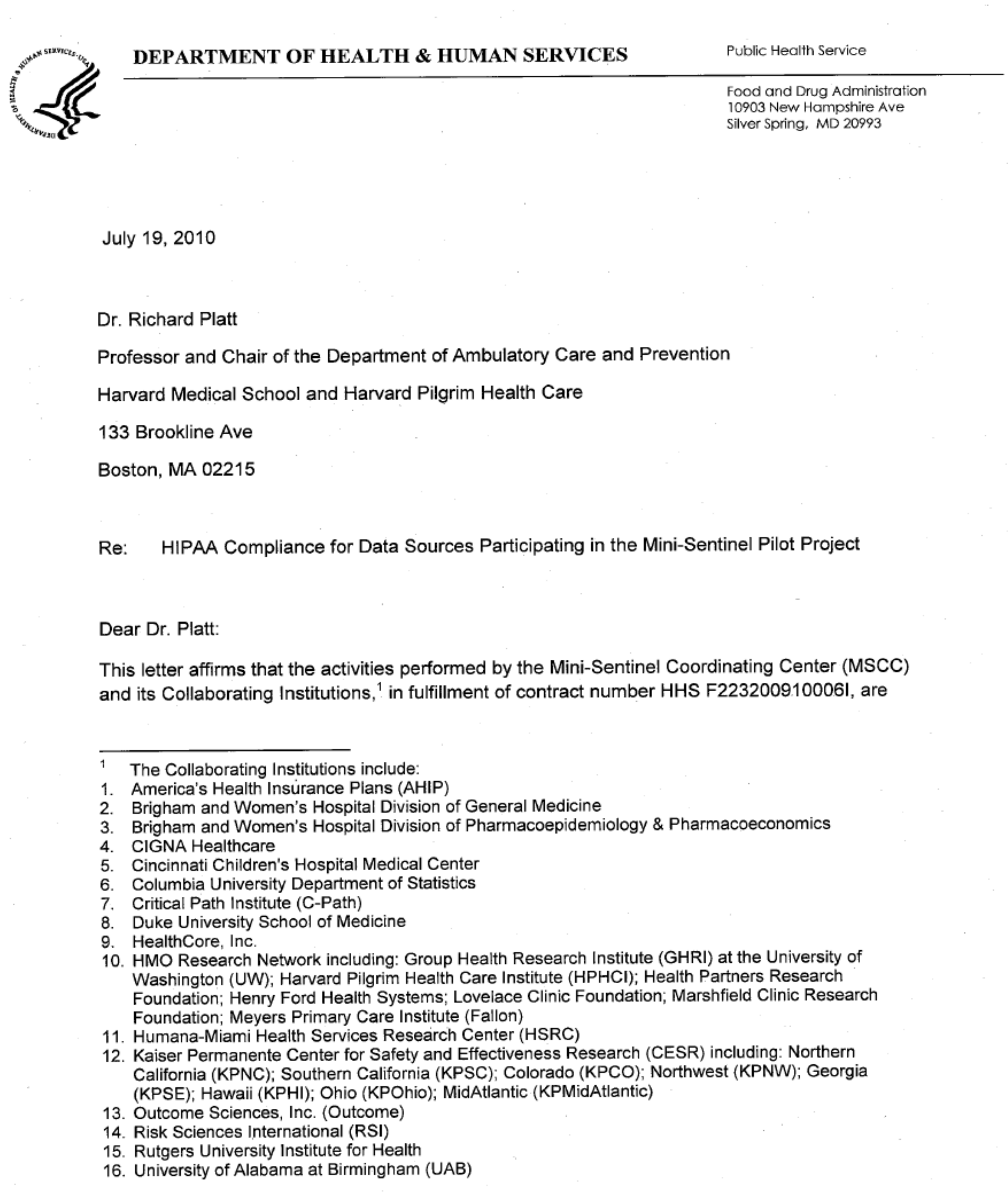
The attached letter from the Office for Human Research Protections states: "The Office for Human Research Protections has determined that the regulations this office administers (45 CFR Part 46) do not apply to the activities that are included in the Food and Drug Administration's Sentinel Initiative."

This assessment applies to the work being conducted by you and your subcontractors under contract number HHSF223200910006I, as the purpose of this contract is to carry out activities that are included in the Food and Drug Administration's Sentinel Initiative.

Please let me know if you have any questions.

Rachel E. Behrman, MD, MPH
Sentinel Initiative, Executive Sponsor

3. Exhibit 3



DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Food and Drug Administration
10903 New Hampshire Ave
Silver Spring, MD 20993

July 19, 2010

Dr. Richard Platt
Professor and Chair of the Department of Ambulatory Care and Prevention
Harvard Medical School and Harvard Pilgrim Health Care
133 Brookline Ave
Boston, MA 02215

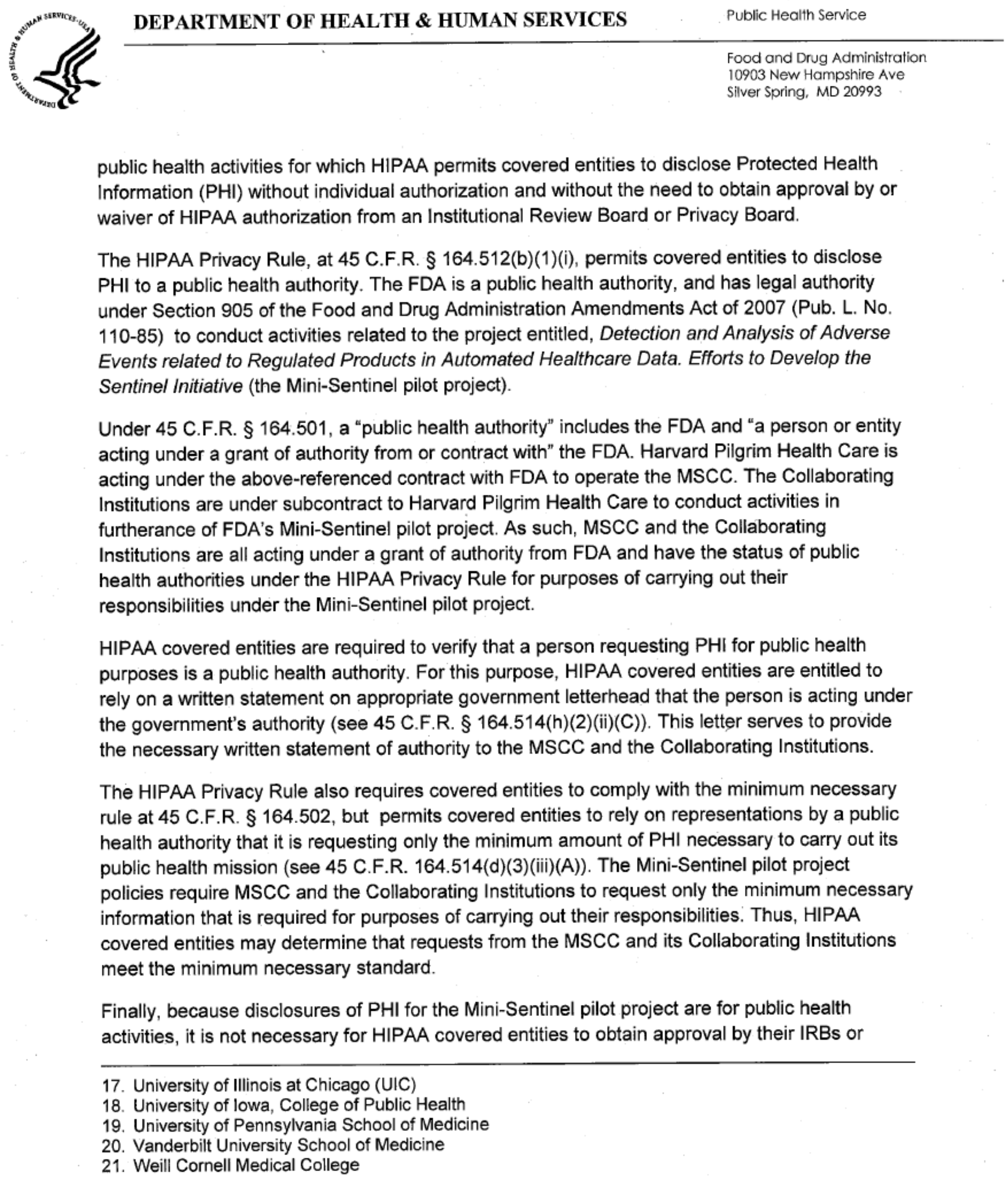
Re: HIPAA Compliance for Data Sources Participating in the Mini-Sentinel Pilot Project

Dear Dr. Platt:

This letter affirms that the activities performed by the Mini-Sentinel Coordinating Center (MSCC) and its Collaborating Institutions,[1] in fulfillment of contract number HHS F223200910006I, are

[1] The Collaborating Institutions include:

1. America's Health Insurance Plans (AHIP)
2. Brigham and Women's Hospital Division of General Medicine
3. Brigham and Women's Hospital Division of Pharmacoepidemiology & Pharmacoeconomics
4. CIGNA Healthcare
5. Cincinnati Children's Hospital Medical Center
6. Columbia University Department of Statistics
7. Critical Path Institute (C-Path)
8. Duke University School of Medicine
9. HealthCore, Inc.
10. HMO Research Network including: Group Health Research Institute (GHRI) at the University of Washington (UW); Harvard Pilgrim Health Care Institute (HPHCI); Health Partners Research Foundation; Henry Ford Health Systems; Lovelace Clinic Foundation; Marshfield Clinic Research Foundation; Meyers Primary Care Institute (Fallon)
11. Humana-Miami Health Services Research Center (HSRC)
12. Kaiser Permanente Center for Safety and Effectiveness Research (CESR) including: Northern California (KPNC); Southern California (KPSC); Colorado (KPCO); Northwest (KPNW); Georgia (KPSE); Hawaii (KPHI); Ohio (KPOhio); MidAtlantic (KPMidAtlantic)
13. Outcome Sciences, Inc. (Outcome)
14. Risk Sciences International (RSI)
15. Rutgers University Institute for Health
16. University of Alabama at Birmingham (UAB)



DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Food and Drug Administration
10903 New Hampshire Ave
Silver Spring, MD 20993

public health activities for which HIPAA permits covered entities to disclose Protected Health Information (PHI) without individual authorization and without the need to obtain approval by or waiver of HIPAA authorization from an Institutional Review Board or Privacy Board.

The HIPAA Privacy Rule, at 45 C.F.R. § 164.512(b)(1)(i), permits covered entities to disclose PHI to a public health authority. The FDA is a public health authority, and has legal authority under Section 905 of the Food and Drug Administration Amendments Act of 2007 (Pub. L. No. 110-85) to conduct activities related to the project entitled, *Detection and Analysis of Adverse Events related to Regulated Products in Automated Healthcare Data. Efforts to Develop the Sentinel Initiative* (the Mini-Sentinel pilot project).

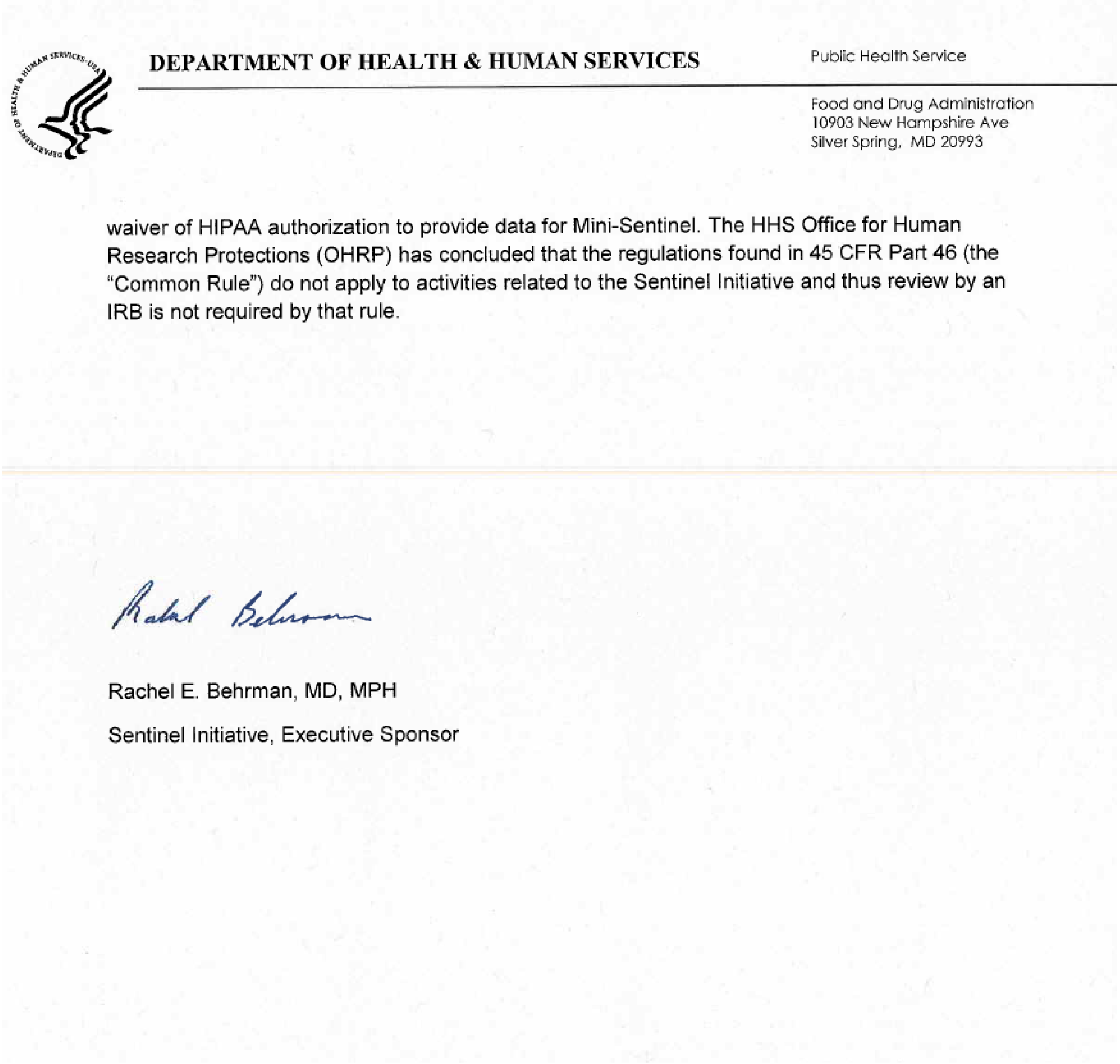
Under 45 C.F.R. § 164.501, a "public health authority" includes the FDA and "a person or entity acting under a grant of authority from or contract with" the FDA. Harvard Pilgrim Health Care is acting under the above-referenced contract with FDA to operate the MSCC. The Collaborating Institutions are under subcontract to Harvard Pilgrim Health Care to conduct activities in furtherance of FDA's Mini-Sentinel pilot project. As such, MSCC and the Collaborating Institutions are all acting under a grant of authority from FDA and have the status of public health authorities under the HIPAA Privacy Rule for purposes of carrying out their responsibilities under the Mini-Sentinel pilot project.

HIPAA covered entities are required to verify that a person requesting PHI for public health purposes is a public health authority. For this purpose, HIPAA covered entities are entitled to rely on a written statement on appropriate government letterhead that the person is acting under the government's authority (see 45 C.F.R. § 164.514(h)(2)(ii)(C)). This letter serves to provide the necessary written statement of authority to the MSCC and the Collaborating Institutions.

The HIPAA Privacy Rule also requires covered entities to comply with the minimum necessary rule at 45 C.F.R. § 164.502, but permits covered entities to rely on representations by a public health authority that it is requesting only the minimum amount of PHI necessary to carry out its public health mission (see 45 C.F.R. 164.514(d)(3)(iii)(A)). The Mini-Sentinel pilot project policies require MSCC and the Collaborating Institutions to request only the minimum necessary information that is required for purposes of carrying out their responsibilities. Thus, HIPAA covered entities may determine that requests from the MSCC and its Collaborating Institutions meet the minimum necessary standard.

Finally, because disclosures of PHI for the Mini-Sentinel pilot project are for public health activities, it is not necessary for HIPAA covered entities to obtain approval by their IRBs or

17. University of Illinois at Chicago (UIC)
18. University of Iowa, College of Public Health
19. University of Pennsylvania School of Medicine
20. Vanderbilt University School of Medicine
21. Weill Cornell Medical College



DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Food and Drug Administration
10903 New Hampshire Ave
Silver Spring, MD 20993

waiver of HIPAA authorization to provide data for Mini-Sentinel. The HHS Office for Human Research Protections (OHRP) has concluded that the regulations found in 45 CFR Part 46 (the "Common Rule") do not apply to activities related to the Sentinel Initiative and thus review by an IRB is not required by that rule.

Rachel E. Behrman, MD, MPH

Sentinel Initiative, Executive Sponsor

VIII. REFERENCES

[1] 2012 HHS PHEMCE strategy and implementation plan. Washington, D.C: U.S. Department of Health and Human Services, 2013. (Accessed February 4, 2014, at http://www.phe.gov/Preparedness/mcm/phemce/Pages/strategy.aspx.)

[2] Dispensing medical countermeasures for public health emergencies: workshop summary, current plans and gaps regarding medical countermeasure dispensing. Washington, D.C.: Institute of Medicine (US) Forum on Medical and Public Health Preparedness for Catastrophic Events, 2008. (Accessed March 8, 2014, at http://www.ncbi.nlm.nih.gov/books/NBK4112/.)

[3] Public Health Emergency Medical Countermeasures Enterprise. Washington, D.C.: U.S. Department of Health and Human Services, 2013. (Accessed February 4, 2014, at http://www.phe.gov/Preparedness/mcm/phemce/Pages/default.aspx.)

[4] PHEMCE mission components. Washington, D.C.: U.S. Department of Health and Human Services, 2012. (Accessed February 4, 2014, at http://www.phe.gov/Preparedness/mcm/phemce/Pages/mission.aspx.)

[5] Barnett DJ, Thompson CB, Errett NA, Semon NL, Anderson MK. Determinants of emergency response willingness in the local public health workforce by jurisdictional and scenario patterns: a cross-sectional survey. BMC Public Health 2012 Mar; 12:164.

[6] Public Health Preparedness Capabilities: National Planning Standards for State and Local Planning. Atlanta, GA: Centers for Disease Control and Prevention, 2011.

[7] Strategic National Stockpile (SNS). Atlanta, GA: Centers for Disease Control and Prevention, 2014. (Accessed March 15, 2014, at http://www.cdc.gov/phpr/stockpile/stockpile.htm.)

[8] Cities Readiness Initiative. Atlanta, GA: Centers for Disease Control and Prevention, 2013. (Accessed July 2, 2014, at http://www.cdc.gov/PHPR/stockpile/cri/index.htm.)

[9] Ball R. Perspectives on the future of postmarket vaccine safety surveillance and evaluation. Expert Rev. Vaccines 2014; 13(4):455-462.

[10] Nguyen M, Ball R, Midthun K, Lieu TA. The Food and Drug Administration's post-licensure rapid immunization safety monitoring program: strengthening the federal vaccine safety enterprise. Pharmacoepidemiology and Drug Safety, 2012; 21(S1):291-7.

[11] Regulatory information. Silver Spring, M.D.: U.S. Food and Drug Administration, 2011. (Accessed April 17, 2014, at http://www.fda.gov/regulatoryinformation/legislation/federalfooddrugandcosmeticactfdcact/significantamendmentstothefdcact/foodanddrugadministrationamendmentsactof2007/default.htm.)

[12] Platt R, Carnahan RM, Brown JS, et al. The U.S. Food and Drug Administration's Mini-Sentinel program: status and direction. Pharmacoepidemiology and Drug Safety, 2012; 21(S1):1-8.

[13] Yi, WK, Sandh, S, Nguyen M, et al. Assessing the freshest feasible data for conducting active influenza vaccine safety surveillance. (Accessed March 2, 2014, at http://www.mini-sentinel.org/work_products/PRISM/Mini-Sentinel_PRISM_Active-Influenza-Vaccine-Safety-Surveillance-Protocol.pdf.)

[14] Nguyen M, Ball R, Midthun K, Lieu TA. The Food and Drug Administration's post-licensure rapid immunization safety monitoring program: strengthening the federal vaccine safety enterprise. Pharmacoepidemiology and Drug Safety, 2012; 21(S1):291-7.

[15] BioSense: public health surveillance through collaboration. Atlanta, G.A.: Centers for Disease Control and Prevention, 2013. (Accessed September 16, 2014, at http://www.cdc.gov/biosense/files/DHIS_BioSense%20Overview_244951_12_3_2013.pdf.)

[16]Coates RJ, Gallagher, K. Use of BioSense for rapid assessment of the safety of medical countermeasures. Online Journal of Public Health Informatics, 2013; S1(5)(1). ISSN 1947-2579.

[17] Vellozi C, Broder KR, Haber P, et al. Adverse events following influenza A (H1N1) 2009 monovalent vaccines reported to the Vaccine Adverse Event Reporting System, United States, October 1, 2009-January 31, 2010. Vaccine, 2010; 28(45):7248-55.

[18] Nguyen M, Ball R, Midthun K, Lieu TA. The Food and Drug Administration's post-licensure rapid immunization safety monitoring program: strengthening the federal vaccine safety enterprise. Pharmacoepidemiology and Drug Safety, 2012; 21(S1):291-7.

[19] Yu Y., Garg S, Yu P, et al. Peramivir Use for Treatment of Hospitalized Patients With Influenza A(H1N1)pdm09 Under Emergency Use Authorization, October 2009–June 2010. *Clinical Infectious Diseases* 2012;55(1):8–15.

[20] The MITRE Corporation. Adverse Events Monitoring and Analysis Proof of Concept Final Technical Report (version 1.2). Task Order No. #HHSF223201310225W. August 19, 2015 (Accessed 9/27/15 at http://www.fda.gov/downloads/emergencypreparedness/counterterrorism/medicalcountermeasures/mcmregulatoryscience/ucm463367.pdf).

[21] Hoyle T, McMahill-Walraven C, Selvam N, Selvan M, Pointon L, Lieu T. Equipping PRISM for pandemic influenza interoperability specification for data partners and immunization registries. (Accessed March 2, 2014, at http://www.mini-sentinel.org/work_products/PRISM/Mini-Sentinel_PRISM_Equipping-PRISM-for-Pandemic-Influenza_Interoperability-Specification.pdf.)

[22] Health IT Regulations: Meaningful Use Regulations. (Accessed November 7, 2014, at http://www.healthit.gov/policy-researchers-implementers/meaningful-use-regulations.)

[23] Hoyle T, McMahill-Walraven C, Selvam N, Selvan M, Pointon L, Lieu T. Equipping PRISM for pandemic influenza interoperability specification for data partners and immunization registries. (Accessed March 2, 2014, at http://www.mini-sentinel.org/work_products/PRISM/Mini-Sentinel_PRISM_Equipping-PRISM-for-Pandemic-Influenza_Interoperability-Specification.pdf.)

[24] Yih WK, Sandhu S, Nguyen M, et al. Assessing the freshest feasible data for conducting active influenza vaccine safety surveillance. (Accessed March 2, 2014, at http://www.mini-sentinel.org/work_products/PRISM/Mini-Sentinel_PRISM_Active-Influenza-Vaccine-Safety-Surveillance-Protocol.pdf.)

[25] Yih WK, Sandhu S, Nguyen M, et al. Assessing the freshest feasible data for conducting active influenza vaccine safety surveillance. (Accessed March 2, 2014, at http://www.mini-sentinel.org/work_products/PRISM/Mini-Sentinel_PRISM_Active-Influenza-Vaccine-Safety-Surveillance-Protocol.pdf.)

[26] Yih WK, Zichittella L, Sandhu SK, Nguyen M, Kulldorff M, Cole DV, Jin R, Kawai AT, McMahill-Walraven CN, Selvam N, Selvan MS, Lee GM. Accessing the Freshest Feasible Data for Conducting Active Influenza Vaccine Safety

Surveillance Final Report. (Accessed May 8, 2015, at http://www.mini-sentinel.org/work_products/PRISM/Mini-Sentinel_PRISM_Active-Influenza-Vaccine-Safety-Surveillance-Report.pdf.)

[27]Goddard K, McClung M, Daley M, Davidson A, Palen T, Nyirenda C, Forrow S, Platt R, Courtney B, Reichman M. Medical Countermeasures Surveillance Field Test. (Accessed TBD pending posting date, at http://www.mini-sentinel.org/work_products/Data_Activities/Mini-Sentinel_Medical-Countermeasures-Surveillance-Field-Test-Report.pdf)

[28] Rosati K, Evans, B, McGraw D. HIPAA and Common Rule Compliance in the Mini-Sentinel Pilot. (Accessed [date] at http://mini-sentinel.org/work_products/About_Us/HIPAA_and_CommonRuleCompliance_in_the_Mini-SentinelPilot.pdf). This White Paper was produced as a general reference source and is not meant to provide legal advice to any person or entity that receives a copy of the work.

[29] 45 C.F.R. § 160.102.

[30] 45 C.F.R. § 160.103.

[31] 45 C.F.R. § 160.103.

[32] 45 C.F.R. § 164.103.

[33] 45 C.F.R. § 160.103 (excluding from the definition of “protected health information,” information in “employment records held by a covered entity in its role as employer.”

[34] 45 C.F.R. § 160.103 (defining “individually identifiable health information” as “information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.”).

[35] *See* Barbara J. Evans, “Congress’ New Infrastructural Model of Medical Privacy,” 84:2 Notre Dame Law Review 586 (2009); James G. Hodge, “An Enhanced Approach to Distinguishing Public Health Practice and Human Subjects Research,” 33 J.L. Med. & Ethics (2005); James G. Hodge, Jr. & Lawrence O. Gostin, Council of State & Territorial Epidemiologists, “Public Health Practice vs. Research,” (2004) (on file with the author); Nat’l Inst. of Health, U.S. Dep’t of Health & Human Servs., “Protecting Personal Health Information in Research (2004), available at http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf ; Paul J. Amoroso & John P. Middaugh, “Research vs. Public Health Practice: When Does a Study Require IRB Review?,” 36 Preventive Med. (2003);); Ctrs. for Disease Control & Prevention, U.S. Dep’t of Health & Human Servs., “Guidelines for Defining Public Health Research and Non-Research (1999) (hereinafter “CDC Guidelines”) (on file with the author); Dixie E. Snider, Jr. & Donna F. Stroup, “Defining Research When it Comes to Public Health,” 112 Pub. Health Rep. 29 (1997).

[36] CDC Guidelines at 24.

[37] *See Ethical Oversight of Learning Health Care Systems,* The Hastings Center (2013) (arguing that the current definition of “research” is unworkable, and that ethics oversight should be provided in accordance with risks to individuals).

[38] CDC Guidelines at 28.

[39] See Appendix B. Exhibit 1.

[40] See Appendix B. Exhibit 2.

[41] Rosati K, Evans, B, McGraw D. HIPAA and Common Rule Compliance in the Mini-Sentinel Pilot. (Accessed [date] at http://mini-sentinel.org/work_products/About_Us/HIPAA_and_CommonRuleCompliance_in_the_Mini-SentinelPilot.pdf). This White Paper was produced as a general reference source and is not meant to provide legal advice to any person or entity that receives a copy of the work.

[42] "Authorization" is a term of art under HIPAA that refers to a permission form with specific elements in it. *See* 45 C.F.R. § 164.508 .

[43] 45 C.F.R. § 164.512(b).

[44] 45 C.F.R. § 164.512(b).

[45] Section 905 of the Food and Drug Administration Amendments Act of 2007 ("FDAAA") called on 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—the Sentinel Initiative. Mini-Sentinel, as a pilot project of the Sentinel Initiative, is intended to provide the foundational work necessary to inform and facilitate the development of a fully operational active surveillance system for monitoring the safety of FDA-regulated medical products. MCM safety surveillance activities fall squarely within the purpose of the Sentinel Initiative, authorized by FDAAA.

[46] 45 C.F.R. §164.501 (defining a "public health authority" as an "agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such 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.") (emphasis added).

[47] See Appendix B. Exhibit 3.

[48] 45 C.F.R. § 164.514(h)(1)(i).

[49] 45 C.F.R. § 164.514(h)(2)(ii)(C) (allowing a covered entity, when making disclosure to a person acting on behalf of a public official, to rely on "a written statement on appropriate governmental letterhead that the person is acting under the government's authority or other evidence or documentation of the agency, such as a contract for services … that establishes that the person is acting on behalf of the public official"); 45 C.F.R. § 164.514(h)(2)(iii)(A) (permitting a covered entity to rely on the written statement of a public agency regarding the legal authority under which it is requesting PHI, or an oral statement if a written statement is impracticable). See also 65 Fed. Reg. at 82547.

[50] See Appendix B. Exhibit 3.

[51] 45 C.F.R. § 164.502(b)(1).

[52] 45 C.F.R. § 164.502(b)(2).

[53] 45 C.F.R. § 164.514(d)(5).

[54] See 45 C.F.R. § 164.514(d)(3)(iii) ("A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose." While §13405(b) of the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), codified at 42 U.S.C. § 17935, contains a provision that requires covered entities to determine what is the minimum amount of PHI for a disclosure, the amendments to the HIPAA Privacy Rule to implement the HITECH Act did not modify a covered entity's ability to rely on minimum necessary representations by public officials. *See* 78 Fed. Reg. 5566 (Jan. 25, 2013), *codified at* 45 C.F.R. Parts 160 and 164, Subpart E.