



Healthcare and Information Management Systems Society (HIMSS)
Public Comment on
Public Docket Number FDA-2008-N-0612: The FDA Sentinel Initiative
(HIMSS Comments noted in blue)
January 16, 2009

1. Governance and Infrastructure

- Who will be responsible for the various aspects of Sentinel, and how will they be coordinated?
 - In FDA's efforts to create a national electronic system for monitoring medical product safety, bodies such as the Joint Commission and the National Quality Forum could be very influential in monitoring participation in, and the effective use of, this system. As health information technology continues to take on an ever-increasing role in the safety, effectiveness, and quality of health-related outcomes, the inclusion of medical product safety as a key evaluation measure for healthcare institutions should take priority, to include the ways that medical devices share data with electronic medical records (EMRs).
- Who will be able to use the Sentinel infrastructure, and under what conditions?
 - The Sentinel infrastructure should be accessible to hospitals, physician practices, and public health entities. Ideally, functionality would be included that enables medical products to automatically generate digital reports via their EMR systems. Incorporation of such functionality through the CCHIT (Certification Commission for Health IT) process would help standardize and infiltrate the Sentinel system throughout the healthcare industry.
 - In addition, it is essential that the Sentinel initiative align with Healthcare Information Technology Standards Panel (HITSP) current and future interoperability specifications that are designed to advance the standard harmonization effort to achieve interoperability of electronic health record systems, allowing advanced versions of the Sentinel initiative to tap information through the Nationwide Health Information Network.
- How will the Sentinel be sustained financially?
 - Financial sustainability should be funded through federal government entities, such as the Department of Health and Human Services.

2. Data and Scientific Operations

- What data are needed?
 - Output from clinical decision support systems will be required that identify changes to the clinical status of a patient that could be associated with the medical device (e.g., patients who are administered Benadryl® after experiencing allergic reaction symptoms; patients who experience abnormal swings in blood pressure or cardiac functions, etc.)

- Whose responsibility is it to ensure privacy is protected?
 - The Sentinel Initiative’s governing body, however it is defined and structured, should take on responsibility for ensuring that privacy is being protected to the maximum extent possible. One approach might be for the governing body to create a Privacy Work Group to identify privacy and security requirements for operation of the Sentinel System. This Work Group could later transition to a monitoring and reporting capability operated by the governing body on an ongoing basis.

With regard to operation of the system itself, each entity that is a participant in / user of the Sentinel System should be required to meet the defined requirements. The Privacy and Security Framework mentioned above contains guidance and specific artifacts to ensure that these controls are implemented, and adherence assured, through appropriate monitoring and other means and methods in order to mitigate non-adherence and breaches. The “Toolkit”² published with the Framework includes sample artifacts such as data use agreements and other tools that can be used in this context. HIMSS recommends that the governing body make use of the framework and toolkit, which have been provided by the Office of the National Coordinator for exactly this type information-sharing system.

² <http://www.hhs.gov/healthit/privacy/framework.html>