Health Information Technology (HIT) Policy Committee
Adoption/Certification Workgroup
February 25, 2010

Testimony of Jeffrey Shuren, Director of FDA's Center for Devices and Radiological Health

Thank you for the opportunity to participate in this Workgroup discussion and share the FDA's perspective on potential approaches to address HIT-related safety concerns. Taking a balanced public health approach, the FDA seeks to support the benefits that HIT can bring through improvements in individual patient care and the overall healthcare system, while also minimizing the risks that this technology can potentially create.

This statement describes: (1) the FDA's legal and regulatory authorities over medical devices and the approach we have taken with respect to HIT to date; (2) various safety issues that have been reported to the FDA and other unique challenges presented by HIT; and (3) possible approaches the FDA could take in the future to help address these concerns.

The FDA's Center for Devices and Radiological Health (CDRH) is responsible for protecting and promoting the public health by assuring the safety, effectiveness, and quality of medical devices – including software devices – throughout the total product life cycle.

Under FDA regulations, medical device establishments must electronically register and list their devices with the agency. Additionally, device manufacturers must submit Medical Device Reports (MDRs), the agency's mechanism for reporting adverse events associated with devices on the market. Manufacturers are required to report to the FDA device-related deaths and serious injuries, and malfunctions that may, if they were to recur, result in death or serious injury. User facilities must report device-related deaths to the FDA and device manufacturers, and must report serious injuries to device manufacturers.

Further requirements apply to certain medical devices based on risk. For example, the FDA requires premarket review of medium- to high-risk devices, such as infusion pumps or heart valves. The agency may also require postmarket surveillance, including post-approval studies or device tracking, for particular types of devices.

To further monitor the safety of medical devices on the market, the FDA also collects information through voluntary reporting programs. Patients and practitioners may voluntarily submit adverse event reports through the FDA's MedWatch system. CDRH's Medical Product Safety Network (MedSun) allows for active surveillance of roughly 350 participating user facilities, all of which receive training in medical device adverse event reporting. Device-related adverse event reports from the MDR system, MedWatch, and MedSun are collected in a publicly available database and are subjected to both routine and ad hoc analyses within the agency. Because our adverse event data is available to the public, members of the private sector and academia may also use it conduct their own analyses and research.

Under the Federal, Food, Drug, and Cosmetic Act, HIT software is a medical device. Currently, the FDA mandates that manufacturers of other types of software devices comply with the laws and regulations that apply to more traditional medical device firms. These products include devices that contain one or more software components, parts, or accessories (such as electrocardiographic (ECG) systems used to monitor patient activity), as well as devices that are composed solely of software (such as laboratory information management systems). To date, FDA has largely refrained from enforcing our regulatory requirements with respect to HIT devices.

Nevertheless, certain HIT vendors have voluntarily registered and listed their software devices with the FDA, and some have provided submissions for premarket review. Additionally, patients, clinicians, and user facilities have voluntarily reported HIT-related adverse events. In the past two years, we have received 260 reports of HIT-related malfunctions with the potential for patient harm – including 44 reported injuries and 6 reported deaths. Because these reports are purely voluntary, they may represent only the tip of the iceberg in terms of the HIT-related problems that exist.

Even within this limited sample, several serious safety concerns have come to light. The reported adverse events have largely fallen into four major categories: (1) errors of commission, such as accessing the wrong patient's record or overwriting one patient's information with another's; (2) errors of omission or transmission, such as the loss or corruption of vital patient data; (3) errors in data analysis, including medication dosing errors of several orders of magnitude; and (4) incompatibility between multi-vendor software applications and systems, which can lead to any of the above.[1]

HIT devices present unique considerations, each of which has the potential to impact patient safety. HIT software applications do not typically operate as stand-alone devices. Instead, these products are interconnected with one another into networks of varying degrees of complexity. Additionally, HIT software is designed to be dynamic and adaptable. User facilities expect to have the ability to make configuration changes to meet their local needs.

The FDA recognizes the tremendous importance of HIT and its potential to improve patient care. However, in light of the safety issues that have been reported to us, we believe that a framework of federal oversight of HIT needs to assure patient safety. Any such framework would need to take into account the complex and dynamic nature of HIT systems. Given the FDA's regulatory authorities and analytical tools, we could potentially, at a minimum, play an important role in preventing and addressing HIT-related safety issues, thereby helping to foster confidence in these devices.

The FDA could consider a range of approaches for addressing HIT-related safety concerns.

One possible approach would be to focus on postmarket safety by requiring HIT device establishments to electronically register and list their HIT devices, and to submit Medical Device Reports (MDRs) to the FDA. Under this approach, HIT device manufacturers would be responsible for correcting identified safety issues. The FDA could also make use of our

[1] For specific examples of reported problems, see the Appendix.

authority to require postmarket surveillance or tracking for selected higher-risk devices, which would provide more detailed information about the use and potential safety risks associated with these products. The FDA could share our postmarket information with vendors, premarket certification bodies, and users to help improve the design of future products. The FDA would exercise our discretion to not enforce other applicable requirements.

A second possible approach would be to focus on manufacturing quality and postmarket safety by requiring HIT device manufacturers to comply with the requirements described above, and also to adhere to FDA's Quality Systems Regulation (QSR). QSR requires manufacturers to adhere to specific minimum guidelines to assure the quality and consistency of products on the market. For example, the regulation requires that device manufacturers establish procedures for handling complaints from users, and for correcting and preventing recurrence of problems.

According to QSR, all software devices must comply with appropriate design controls to reduce the potential for problems. Design controls are an interrelated set of practices and procedures that are incorporated into the design and development process of a device, in order to check for problems and make corrections in the design of the device before it is put into production. For example, manufacturers of software devices must establish and maintain procedures for verification and validation of their device design. Based on data collected through our postmarket safety authority, the FDA could recommend design controls that would mitigate the risks that are unique to HIT devices, such as those associated with multiple software products interfacing with one another as a part of a comprehensive HIT system, or those associated with user-facility-specific customization of HIT software after installation. Such design controls would help to preserve the ability of user facilities to innovate and tailor the installation and use of these devices to their practical needs, while reducing risks to patients. The FDA would exercise our discretion to not enforce other applicable requirements.

Under a third approach, the FDA would apply our traditional regulatory framework, in which HIT device manufacturers would be required to meet all the same regulatory requirements as other, more traditional devices, including risk-based premarket review. Through premarket review, the FDA could assess the safety and effectiveness of high- and medium-risk HIT devices before they go into market use. Additionally, the FDA could establish certain requirements for approval for selected products. For example, the FDA could require that manufacturers provide as prerequisites for approval a clear installation plan for a given HIT device, or a hazard analysis of risk associated with medical-facility-specific configuration. The FDA could also require postmarket studies or specific product labeling for particular HIT devices as conditions for approval.

By working both collaboratively with and in complement to our government partners, the FDA could help to mitigate risks to the public health while promoting innovation.

Appendix: Examples of Reported Adverse Events

Category	Examples
Errors of Commission	**Example 1:** An error occurred in software used to view and document patient activities. When the user documented activities in the task list for one patient and used the "previous" or "next" arrows to select another patient chart, the first patient's task list displayed for the second patient. **Example 2:** A nuclear medicine study was saved in the wrong patient's file. Investigation suggested that this was due to a software error. **Example 3:** A sleep lab's workstation software had a confusing user interface, which led to the overwriting and replacement of one patient's data with another patient's study.
Errors of Omission or Transmission	**Example 1:** An EMR system was connected to a patient monitoring system to chart vital signs. The system required a hospital staff member to download the vital signs, verify them, and electronically post them in the patient's chart. Hospital staff reported that, several times, vital signs have been downloaded, viewed, and approved, and have subsequently disappeared from the system. **Example 2:** An operating room management software application frequently "locked up" during surgery, with no obvious indication that a "lock-up" was occurring. Operative data were lost and had to be re-entered manually, in some cases from the nurse's recollection. **Example 3:** An improper database configuration caused manual patient allergy data entries to be overwritten during automatic updates of patient data from the hospital information system.
Errors in Data Analysis	**Example 1:** In one system, intravenous fluid rates of greater than 1,000 mL/hr were printed as 1 mL/hr on the label that went to the nursing / drug administration area. **Example 2:** A clinical decision support software application for checking a patient's profile for drug allergies failed to display the allergy information properly. Investigation by the vendor determined that the error was caused by a missing codeset. **Example 3:** Mean pressure values displayed on a patient's physiological monitors did not match the mean pressures computed by the EMR system after systolic and diastolic values were entered.

Category	Examples
Incompatibility between Multi-Vendor Software Applications or Systems	**Example 1:** An Emergency Department management software package interfaces with the hospital's core information system and the laboratory's laboratory information system; all three systems are from different vendors. When lab results were ordered through the ED management software package for one patient, another patient's results were returned. **Example 2:** Images produced by a CT scanner from one vendor were presented as a mirror image by another vendor's picture archiving and communication system (PACS) web software. The PACS software vendor stipulates that something in the interface between the two products causes some images to be randomly "flipped" when displayed.