HIT Policy Committee
Adoption/Certification Workgroup

Omni Shoreham Hotel, 2500 Calvert Street, NW, Washington, DC

Thursday, February 25, 2010, 9 a.m. to 3:00 p.m./Eastern Time

Panel II: Stakeholders

Developing an Electronic Health Record (EHR) Patient Safety System

Good morning. I am Jean M. Scott, MT (ASCP) – Director of the Veterans Health Administration's Information Technology Patient Safety Office. I would like to thank the co-chairs, Paul Egerman and Marc Probst, and the members of the committee for the opportunity to represent the Department of Veterans Affairs (VA) in this important conversation convened by the HIT Policy Committee's Adoption and Certification Workgroup.

By 1985 most VA medical centers (VAMCs) had implemented the Veterans Administration Decentralized Hospital Computer Program (DHCP), a simple character user interface to automate capture and viewing of health information. Today DHCP is now only one part of the overall information resources at the local facility level. Since 1996, VA's electronic health care system, now known collectively as Veterans Information System Technology Architecture (VistA), provides an integrated inpatient and outpatient electronic health record and the administrative tools to deliver Veterans quality medical care. VistA is composed of over 100 software components, including a clinician facing system known as Computerized Patient Record System, or CPRS. VistA incorporates all of the benefits of DHCP as well as including the rich array of other information resources that are becoming vital to the day-to-day operations at VA medical facilities. VA's health care system includes 153 medical centers, with at least one in each state, Puerto Rico, and the District of Columbia. VA operates more than 1,400 sites of care, including 909 ambulatory care and community-based outpatient clinics, 135 community living centers (nursing homes), 47 residential rehabilitation treatment programs, 232 Veterans Centers and 108 comprehensive home-care programs. VA health care facilities provide a broad spectrum of medical, surgical, and rehabilitative care.* In support of our nation's Veterans, VistA has recorded more than 2 billion patient orders, documented administration of more than 1.1 billion medications, and provided access to more than 1 million images.

VA recognizes the need to have a comprehensive Information Technology (IT) Patient Safety program integrated with the overall patient safety culture. VHA's IT Patient Safety program began as a collaborative effort in 2002 among the National Center for Patient Safety (NCPS) and the Office of Health Information (OHI). Early reporting was performed using a simple policy by which health IT staff was required to notify senior management upon identification of an issue. It quickly became apparent that a more structured tracking and analysis process was needed and, during the next two years, VA continued with developing a systematic process. Over this time period, several hundred reports were captured and analyzed. Early reporting focused on incident reporting. However, as awareness of a safety culture grew, emphasis was placed on reporting close calls, and the rate of reporting significantly increased. Multiple avenues for reporting IT

safety concerns are now available. Although IT issues are occasionally identified through a Root Cause Analysis (RCA) of a patient event, the majority of IT reporting is presented through the local and national IT Help Desk system(s). IT Specialists are provided education to patient safety concepts and the reporting of close calls. Additionally, reporting methods include the direct incorporation of data entry fields for patient safety flagging into the IT help desk ticket, as well as a web portal for reporting IT patient safety concerns. As a result of early data collection, VHA's IT Patient Safety program is now a fully integrated program office managed by a full-time director that includes health care professionals from several disciplines along with human factors engineering staff.

Reporting of IT patient safety concerns was only the initial step towards establishing patient safety concepts in the IT realm. As the program evolved to encourage close call reporting, the need arose to establish risk evaluation criteria and method to inform clinical users of risks. IT Managers experiencing resource demands from multiple avenues need to understand the urgency of particular issues. Patient Safety evaluation criteria, based on risk assessment principles, should assess the potential impact to patient, frequency of event, and the ability of the user to identify the risk. With information obtained from the IT Managers and their ability to address the software in a timely manner--usually with the release of a patch—the assessment criteria is also used to determine the need to notify clinical users as well as senior leadership. Notification to clinical users is based in the same safety reporting system for other patient safety reporting. IT Safety Reporting is coordinated and jointly decided with NCPS to determine the most appropriate distribution level. Electronic medical record notices involving CPRS and even Bar Code Medication Administration (BCMA) are often distributed via the VHA Safety Alert system. Other types of patient safety concerns are evaluated for which user group (pharmacist, radiologist, laboratories, etc.) are specifically targeted for notification.

The VA Experience – Issues Identified

IT Patient Safety reported cases have been associated with quality defects and design induced error. Safety reporting during 2002 identified defects in software programming logic and data storage that produced erroneous data displays and inaccurate data. In a widely-publicized October 2008 event, VA experienced a software programming defects with the release of CPRS version 27. The defect was identified by a clinician, such that when the clinician accessed a different patient's electronic medical record, the prior patient's data would still be displayed. The defect was thought to be rare, and several attempts to replicate it prior to release were unable to find the cause. Shortly after full release, reporting via the IT Patient Safety channel identified an increased occurrence rate among at least four additional medical facilities. VA issued a patient safety advisory describing the issue and encourage immediate reporting to the national software team. Within three days of the notice, VA had received over 20 additional reports. With the assistance of the IT Patient Safety staff, the software development staff was finally able to isolate the particular sequence of events to replicate the issue, and a remedy was issued within a matter of weeks of the notice. The wide dissemination of the safety advisory was indeed a benefit to timely resolution of the defect.

In addition to issues traditionally defined as software defects, VA has identified many user interface designs that potentially may induce clinical errors. Beginning in 2003, VA received a report of a medication error associated with a sound alike medication. The CPRS software design for medication ordering was originally designed to minimize keystrokes and mouse clicks. The user could simply type the first three characters of a medication name and upon finding any entry that began with those characters the software would auto-highlight the entry for selection. This auto-highlight could be then quickly selected by use of the Enter key. The auto-highlight selection would also predispose the user to select the highlighted entry over another entry in the list. A non health information technology (HIT) example of this design feature can be found in Microsoft™ Outlook when a user types in an e-mail address. The initial report to the potential for patient safety risk was dismissed by the clinical community as "user error" and "re-training" the user was the "solution". The ability of VA to capture multiple reports of the same problem, along with a search of the NCPS database for look-alike/sound-alike medication errors, was the evidence needed to finally enact a change in design. The CPRS user can still type three characters to search for a medication; however the software no longer preselects any entry from the list and requires the user to explicitly select the intended medication. Since release of the software design change in 2005, the IT Patient Safety office did not receive reports of medication errors associated with induced selection.

While the medication ordering design was eventually changed, VA continued to find similar issues in other software initially designed for speed and minimal user keystrokes. Recognizing that designing for default behavior can lead to enhanced adoption of electronic medical records, first and foremost, the system must emphasize the criticality for accuracy in the associated user task. Early systems contained features requested by a user-centered design approach. User-centered design can indeed provide the basis for an ease of use, but an organization must be cognizant of the Human-Centered Design limitations. Critical tasks must be balance not only for speed and adoption of the IT tool, but for accuracy of the task ultimately accomplished. This may involve a perceived sacrifice of speed or ease of use with the ability to satisfy the need for critical task accuracy.

Another spectrum for IT Patient Safety experiences involves identification of multiple mental models and various information systems associated with the information derived from shared data elements. Medication management involves, at minimum, the ordering provider, the processing pharmacist, and the administering nurse. Each of these entities depends upon the same basic data elements associated with the medication such as name, dosage, route of administration, and schedule. One close call involving a medication infusion order revealed the lack of a discrete medication route data field within the provider interface, such that the ordering provider entered infusion routes as free-text based comments. If the pharmacist did not notice the comments, and explicitly edit the route, the pharmacy software defaulted to intravenous (IV) route, while further along the chain; the BCMA software only displayed routes that had defined abbreviations.

The series of both missing data and design defaults increased the vulnerability that an infusion would be assumed to be IV by both pharmacy and nursing staff. Investigations of the entire medication ordering process by the IT Patient Safety program lead to corrective actions in all three related information systems. As this demonstrates, a safety issue may be initially identified

in a single information system at the end point of the error; however one must trace back to the origin and determine whether multiple data points contributed to the chance for error.

Additional sources of potential error are the various integrated user interfaces made available to the clinical user. In some instances, patient demographics will contain full identity trait such as medical record number, name, or date of birth, while other systems will only display partial data. To further complicate use, the screen location and relative size of the patient identity information may vary from system to system. Certain design guidelines may need to be investigated to encourage a standard geographic layout of key patient identity information.

Finally, the occurrence of pop-up fatigue is prevalent among components of the EHR. Clinicians are presented with pop-ups, the design intention of which is to provide decision support, but do not have the ability to address the nature of the pop-ups. A pop-up may also contain a defaulted override feature that contributes to provider ignoring the clinical relevance. By simply accepting the default, the provider is able to continue with the intended task, and has not appropriately addressed the pop-up's intent. Pop-ups are interruptive by nature; however when a pop-up does not allow the user to select an alternative path and forces the user to back out of the task, the pop-up decreases in its significance and contributes to inappropriate overrides.

The examples described represent a subset of the myriad of issues reported with the use of HIT. Both technical and design issues will arise with the use of technology and the integration of multiple complex systems such as those found within health care.

Patient Safety Impact of EHR Use

VA has achieved a level of excellence associated with the ability of information technology to bring rapid decision support and information access to health care providers. The use of HIT reduces certain cognitive burdens associated with medication ordering such as drug-drug and drug-allergy interactions. The ability of the EHR to access vast patient data provides clinicians with the tools to minimize many sources of clinical error. The computer can more easily calculate data interactions and provide early intervention displays that were often not possible with paper-based records. When the EHR is not available, VA clinicians are subjected to contingency planning such as delaying elective care. Clinics may cancel appointments until such time the electronic data is available. Reliance on access to the EHR to provide decision support changes the manner in which clinicians will expect to deliver safe health care. The EHR infrastructure for technology and resource support must be implemented such to minimized EHR downtime. Organizations can expect a direct impact to health care delivery when access to the EHR is not available.

Incorporating Safety into HIT

Reporting of concerns, such as errors and close calls, must be a continuous process, not only during initial implementation, but throughout use of the product. Clinical users will find innovative uses for HIT. It is through this innovative and creative use of HIT that new

vulnerabilities are discovered. Issues may be latent for years or not identified as perceived risks, however as use increases or the clinical setting morphs, the product may no longer be able to address gaps in functionality and lead to increased risk for adverse event. Building on the concepts of aviation safety reporting and a patient safety culture, EHR safety reporting should encourage reporting of close calls.

While certain IT products are currently considered medical devices, there appears to be narrow definition of what is considered a reportable event by the IT device manufacturer. Although VA has adopted a transparent system for reporting and addressing EHR patient safety risks, there is yet more to be accomplished. Patient safety identified risks are not isolated events, but part of a complex system. Early success has been achieved by recognizing HIT as a safety risk in the same realm as Patient Falls, Suicides, Surgical and Medical errors, and applying the same patient safety culture to information technology. **Health care organizations must be able to openly report safety concerns. Reporting should encourage not only sentinel events and defect reporting, but the ability to share EHR safety concerns to identify potential sources for medical error.**

Requiring usability as part of a certification process may make adoption easier; however the goals of usability must be openly stated. Usability may be misconstrued as ease of use. Usability goals must be goal-oriented to ensure accurate task completion. Errors can be prevented by undertaking not only a user-centered design approach, but incorporating human-centered limitations into the design. Private and in-house EHR manufacturers should be able to demonstrate the ability of the product to meet accepted task goals that are based on accuracy of clinical task.

VA has been successful in mitigating risks through open reporting. Some challenges remain as vendor products are incorporated into the VA suite of EHR tools. Issues may be directly reported to the vendor by the individual facility, and other facilities may not be made aware of the vulnerability. This is a challenge that VA's IT Patient Safety office has identified. One proposed avenue to be explored is to require regular reports to the customer or provide the customer with open access to review reports. At a minimum, the health care facility parent organization should be provided access to view reports from its constituent facilities. The ability to mitigate risk comes from a collaborative agreement between the IT teams and the health care organization. The health care system needs to be aware of methods for interim risk mitigation such as limited use of a product.

In addition to reporting identified issues, the health care entity must anticipate unknown safety issues with upgrades and/or disseminated use. VA has recognized that increased vulnerability to new safety risks is associated with major releases. Processes to monitor and have rapid resources available are one method to mitigate safety issues. VA monitors which facilities have installed upgrades and is able to readily notify those at risk, while preventing further risk exposure by also communicating adjustments for additional facility installations.

In summary, an open reporting system that provides feedback will foster a collaborative environment between the HIT and health care communities.

This ends my statement. I want to thank the chairs and the members of the committee for the opportunity to speak on this important topic.

*Source: NATIONAL CENTER FOR VETERANS ANALYSIS AND STATISTICS "VA STATS AT A GLANCE – FEBRUARY 2010":
http://www1.va.gov/vetdata/docs/4X6_winter10_sharepoint.pdf