OFFICE FOR
OREGON HEALTH
POLICY & RESEARCH

DRAFT

OREGON HEALTH CARE QUALITY CORPORATION
A nonprofit partnership for quality improvement

Electronic Health Information Exchange
Critical Issues

The health care environment is changing: electronic medical records are replacing paper records and health information is increasingly being exchanged electronically. While the technology to do this is emerging, there is still a great deal of work to be done to allow for a smooth transition into this new world. Multiple high-profile inappropriate disclosures have heightened consumer concern for the privacy and security of their electronic health information. To function in this new environment, we must build relationship and trust between patients, providers, and other individuals and organizations involved in health care. We must balance the need to protect individuals' privacy with the need to share individuals' health information so that care is safe, effective and efficient.

Accessing Information

Patient Involvement
With increasing exchange of health information in an electronic environment, patients have the opportunity for easier access to their health information, to better understand it and be involved in its uses. This electronic environment also results in heightened concerns about inappropriate disclosure. One of the most challenging issues is defining the patient role in accessing and directing the use of their health record.

- *Patient access to record*
  How can we help patients access, understand and assure the correctness of their health records? How can we assure this works for patients of all backgrounds and abilities? How much access should patients have to their health information? Should there be exceptions?

- *Patient control of access by others*
  What is the patient's role in determining his/her participation in community-wide health information networks? Will this role require changes in the "Notice of Privacy Practices" or the way it is implemented?

Patient identification
In an electronic environment providers may have access to many patient health records, allowing for the sharing of the most timely health information to improve health outcomes. Access to a large repository of information may also increase the likelihood of duplicate names requiring the provider to look at multiple records to identify which is the correct one. How can correct patient identification be ensured without inappropriate disclosures?

Authentication, authorization and access control
To protect the privacy and security of health information it is necessary to ensure that only the appropriate people have access to only the appropriate information. The complexity of this task is magnified in a health information exchange network. In such a network, it is necessary (1) to authenticate that a person who desires access is who he or she claims to be, (2) to establish that

the person has the authority to access the network, and (3) to limit his or her access using role-based controls. How would an authentication and access system work in Oregon? How do we apply the concepts of role-based access in an environment of health information exchange?

Circle of care
With improved access to information, patients may experience improved coordination of care. Protections must be in place to ensure that only those individuals involved in the patient's care can access personal health information. How should circle of care be defined? How should circle of care access be kept up-to-date so that only those individuals currently involved in the patient's care have access to patient's health information? What are the implications of "push" information sharing, when providers are automatically notified of information (e.g. lab results forwarding), versus "pull" information sharing, when providers must request information?

Proper use
Health information exchange increases the ease with which information can flow within an organization and between organizations. This allows for better efficiency and quality of care. However, it also increases the number of potential viewers of the information and the amount of information viewers can access. How can patients be sure that only appropriate people can access their records? How can they be sure that viewers see only the minimum necessary information?

Secondary use
Electronic health records have the potential to provide public good by facilitating access to health information for the purposes of public health reporting, bioterrorism event monitoring, disaster preparedness, health care quality improvement support, and research. What kind of information should be shared for non-treatment purposes? How should this sort of use be authorized and managed?

Protecting Information

Specially protected information
Oregon laws about specially protected health information (i.e. related to minors, substance abuse, mental health, HIV status, and genetic information) create a secondary layer of caution (beyond HIPAA) for sharing sensitive information. Oregon's providers vary widely in their interpretation of when and how to share specially protected information. Are the laws and protections as written suitable and sufficient in an electronic environment? How can we reduce variation in the ways these laws are applied? Should all health information be protected equally?

Redacting
In an electronic environment the ability to redact specially protected information from a health record is more complicated than in a paper world. How will personal health information be protected from improper sharing when health records are sent electronically?

Assuring an accurate, current record
Health status and treatment plans are constantly changing. Information about a patient's health may come from a variety of sources. How can we take advantage of the capabilities of electronic health information exchange to ensure that health records are up-to-date and accurate? How should we define what is relevant and important to a health record? How does a patient or legal representative amend a record? How can we ensure that if amendments or updates are made to the health record, these changes are reflected in all copies of the record?

Data transmission security
Electronic health information exchange will allow providers to send and review health information more easily, both internally and externally. Patients changing doctors or seeing specialists will no longer experience delayed care while waiting for records to be sent. What minimum standards need to be developed to ensure the technical security of electronic transmissions of health information? How can such standards be enforced? How do we assure all of Oregon's providers can appropriately participate regardless of their level of IT implementation?

Tracking access and audit trails
As health information is increasingly available electronically, it is important to do as much as possible to prevent the information from being inappropriately accessed or shared. However, in the event a breach of security does occur, it is essential to have a robust system of audit trails to track access to a patient's record so that appropriate steps can be taken to ensure the inappropriate access is detected and does not reoccur. What standards surrounding maintaining audit trails are needed? How can we learn from mistakes and continually improve the security protections of health information?

Accountability Concerns

Increased liability
Improved health information exchange may result in large quantities of patient health information being sent to providers without an immediate tie to a visit for diagnosis and treatment. Will increased provider liability result from the creation of more information than can be reasonably used? Will healthcare organizations also experience greater liability? How should we address issues that arise from having too much information?

Need for effective sanctions
In order to assure the public trust in healthcare organizations' ability to appropriately protect personal health information, a universal standard of accountability needs to be applied for individuals and/or organizations that violate the privacy and security of electronic health information. How can this be ensured? What are other ways to ensure the public trust? Despite all safeguards to protect security and privacy of health information, inappropriate disclosures will inevitably occur. What should happen when inappropriate disclosure (inadvertent or intentional) occurs? Who is responsible?

Medical identity theft
Increased flow of electronic health information could potentially create greater opportunity for identity theft, including medical identity theft. While the public has long been aware of the potential of financial identity theft, medical identity theft is only now beginning to receive attention. It occurs when someone uses a person's name and/or other parts of their identity – such as their insurance information – to obtain or make false claims for medical services or goods. How can patients be assured that healthcare organizations protect their health information from this threat? How can we ensure that health care organizations are responsive to the needs of medical identity theft victims?

For more information, contact Summer Boslaugh, MBA, MHA, *Project Manager*
503-241-3571, summer.boslaugh@state.or.us

Updated on 12/18/2006