"MINIMUM NECESSARY":
Proposed definitions for Public Health regarding electronic access to patient data
Draft 3/30/2011 for CCLHO HIE Toolkit for Local Health Departments

The general principal of electronic health information exchange is to share the "minimum necessary" information to minimize the exposure of data, thus limiting and containing exposure and issues regarding privacy and security. Thus far there is apparently no standardized definition of "minimum necessary or minimum data set" regarding exchange of health data for public health purposes (Direct patient care and determination of minimum necessary will not be considered here). The HIPPA Privacy Rule permits a covered entity to rely on the determination and judgment of the party requesting the disclosure as to the minimum amount of information needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by a public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).

Providers are required to monitor access and disclosure of health data under their control. Most hospital HIT systems have this capacity, but due to the limitation of embedded security features and the number of transactions occurring daily, they struggle to monitor access proactively. If a breech is suspected, monitoring can occur retrospectively. In general, access to patient data in hospital systems is limited to "the physician (or provider) of record" and access is granted accordingly. In many instances, when Public Health is responding to a mandated report of a public health condition, Public Health Staff are excluded from access because they are not "providers of record," have not ordered the test or admitted the patient and are not listed as the primary care provider in the intake process.

Lacking generally accepted definitions for "minimum necessary" regarding Public Health access to electronic data, Public Health Officers (or staff) negotiate with hospitals to permit Public Health access as "provider of record" and define what is "minimum necessary" in a variety of scenarios.

CASE MANAGEMENT OF REPORTABLE CONDITIONS: One proposal is for the Confidential Morbidity Report (CMR) to trigger public health access. In such a scenario, the hospital would permit the appropriate Public Health Staff member to pre-register for electronic access, just as providers on the medical staff do. This would facilitate on-going monitoring of appropriate usage if desired. In some instances registering Public Health Staff for electronic access might require a change to the hospital bylaws. Thereafter, the Infection Control Practitioner submitting a CMR, or other pre-designated person at the hospital notified by the Infection Control Practioner, could enter the registered Public Health Staff as a "provider of record" in the hospital system, understanding that the Public Health Staff would limit review of the patient's record to information needed to complete the required case reporting to the California Department of Public Health (CDPH) and the Center for Disease Control and Prevention (CDC) when appropriate. Reporting may require more information than is included on the CMR.

Additionally, some conditions reported by CMR may require case management by Public Health Staff. For example, Public Health Staff may need to assure that a tuberculosis patient is receiving optimal

---

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_015785.hcsp?dDocName=bok1_015785

care even in instances when Public Health is not providing direct patient care. In such instances, Public Health Staff would need access to the full medical record including occupation, housing situation, insurance status and ongoing clinical reports.

In order to promote cooperation, hospital HIPAA and medical records staff should be introduced to existing Public Health HIPAA policies, including training programs and sanctions for staff found to be in violation. Hospitals have expressed concern that they have no means to sanction Public Health Staff that do not have clinical privileges. Public Health Staff may decide to track their access to medical record data in a secure manner to be prepared should an audit be initiated.

CONTACT INVESTIGATION: In some instances, a CMR for one patient may trigger public health investigation of that patient's contacts, either as a potential source of the condition or as someone susceptible to disease and in need of prophylaxis or monitoring. In such cases, the Public Health Staff could define the **"**trigger**"** as the need for contact investigation and contact the hospital Infection Control Practitioner (or other pre-designated hospital contact) and request status as "provider of record." Again, the agreement is that Public Health Staff would access the "minimum necessary" data, recognizing that in some instances that may include the entire chart.

SYNDROMIC SURVEILLANCE AND BIOMONITORING: Syndromic surveillance and bio-monitoring for public health purposes are recognized as activities allowable under HIPAA and are incentivized under the HITECH Meaningful Use program. Syndromic surveillance may be as general as delayed reporting by emergency rooms, outpatient providers or hospitals of contacts with patients with certain symptoms, such as influenza-like illness. In such situations it is not necessary to identify individual patients. Nevertheless, such an arrangement would most likely entail a Confidential Data Sharing Agreement or other such contract between Business Associates.

There is growing capacity and interest in refining surveillance activities, including GIS mapping. Specificity of mapping (i.e. state, county, zip code, census track) and monitoring may require Public Health Staff to access address information, which could identify an individual even if it is possible to share address information without a name attached. "Minimum necessary" would depend on the goals of the monitoring project under consideration. Public Health has the capacity to securely receive and store patient-identified data and strip it of personal identifiers, releasing reports refined to a level where identification of individuals involved would not be possible. Such projects might be handled with confidential data sharing agreements or even be submitted to a Human Subjects Review Board for approval.

In some instances of bio-monitoring, it might be compelling to "break the glass" and contact an individual with a condition of particular significance, such as identifying an anthrax case as a matter of national security.

PUBLIC HEALTH REGISTRIES INCLUDING IMMUNIZATION REGISTRIES: Electronic submission of patient data to public health registries is a requirement of the HITECH Meaningful Use Program. It is anticipated that issues of consent and definitions of "minimum necessary" will be determined on a state-wide basis.

---

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_015785.hcsp?dDocName=bok1_015785