Data Usage Controls
Sharing Information and Complying with Confidentiality Constraints through a Virtual Information Service

Eileen Griffin
Institute for Health Policy
Edmund S. Muskie School of Public Service
96 Falmouth Street
P.O. Box 9300
Portland, Maine  04104-9300

February 17, 2005

This report was funded under a cooperative agreement between the University of Southern Maine and the Maine Department of Health and Human Services.
Data Use Controls

Table of Contents

Acknowledgments................................................................................................................ i
Data Usage Controls ............................................................................................................. 1
  Types of Information to be Exchanged................................................................................ 1
  Confidentiality Constraints ............................................................................................... 2
Data Use Controls ............................................................................................................... 5
Conclusion ............................................................................................................................. 6
Acknowledgments

Much gratitude is extended to Dennis Tan and Cathy McGuire who both provided their expertise and guidance in the development of this report.
Data Usage Controls

The work described in this report builds upon work done under the Data Integration project under Quality Choices for Maine. Quality Choices is the Real Choices Systems Change grant from the Centers for Medicare and Medicaid Services to the Department of Health and Human Services. Under the Data Integration project, a design for an Integrated Data Application (IDA) was developed. The proposed IDA would offer a central reusable and extensible infrastructure for integrating information systems across multiple state agencies and data sources. This design is premised upon the ability to translate into electronic process management rules an agreement between a data contributor and a data user that governs the conditions under which data is to be disclosed. The purpose of this project was to explore the types of controls and the procedures needed to ensure that the sharing of information complies with federal and state law. The report below describes the types of information potentially to be exchanged, typical confidentiality constraints on the exchange of information, the potential elements of memoranda of understanding, and the electronic tools that support the electronic exchange of information with appropriate controls.

Types of Information to be Exchanged

State agencies need to share two types information:

Operational data. Operational data is used for serving individual consumers. Operational data is typically individually identifiable. Examples of how interdepartmental data could be used to improve client service include:

- Enrollment and eligibility determination (e.g., to speed enrollment and eligibility determination, an enrollment specialist or other intake worker could automatically populate an enrollment form with the most recent pertinent information, to be confirmed with the individual).
- Service coordination (e.g., a case manager could identify other providers and services, to identify gaps in services and to facilitate communication and coordination among providers).
- Utilization review (e.g., an agency might want to know whether another department or school is funding the same or similar service; whether there is a pattern of overutilization or underutilization; whether care has been appropriate, based on indicators of success or failure, such as repeat returns to treatment or correctional facilities, or successful return to school).

Analytical data. Analytical data is used to support policymakers in making decisions about the most effective use of resources, etc. Analytical data is aggregate, non-identifiable and needs to be representative of the population group being analyzed (i.e., access to analytical data cannot be conditioned on individual authorization).
Examples of how interdepartmental data could be used to support policymaker decisions include:

- **Performance measures** (e.g., different departments and agencies might have an interest in measuring the well-being of the people they serve based on their performance in school, whether or not they are employed, or whether they have come within the jurisdiction of the Department of Corrections).

- **Compliance** (e.g., a department might need to assess whether or not it is complying with a legal mandate such as a requirement to provide a certain service to all individuals having a certain set of characteristics).

- **System capacity** (e.g., a department might want to know how many people on waiting lists are receiving substitute services from another department);

- **Resource management** (e.g., departments might want to identify the characteristics, service needs and utilization patterns of their high-end users to identify appropriate interventions for improving the effectiveness of services);

**Confidentiality Constraints**

When most people think about laws governing the confidentiality of information, they think of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a federal statute that governs the sharing of protected health information, whether the protected health information is held by private or public parties. HIPAA applies to Medicaid data and other health information held by DHHS and other state agencies.

In addition to HIPAA, other federal and state laws govern the protection of individually identifiable information held by the government. For example, federal law governs the protection of Medicaid information, educational records, and substance abuse treatment. State law governs the protection of mental health information and information about persons served by the Department of Corrections. Some of these protections will overlap in scope with HIPAA. Often, relative to these other laws, HIPAA is more comprehensive in its scope and more specific in its application. However, contrary to popular belief, HIPAA is not necessarily the most restrictive law governing information exchange. For example, HIPAA permits a covered entity to disclose protected health information to a business associate for the purpose of electronically linking the information and converting the information to aggregate, de-identified data no longer requiring protection. Many other regulatory schemes were written before the electronic exchange of information and do not so readily accommodate the linking and de-identification of data.

While confidentiality statutes and regulations offer different levels of protection to different types of data owned or created by different types of entities, these laws have many common features. In general, confidentiality statutes will incorporate some or all of the following elements:
The definition of protected information. The information protected will vary. Under HIPAA, protected health information includes individually identifiable health information created or received by a health plan, health provider or health care clearinghouse. Federal Medicaid regulation protects individually identifiable information collected in connection with the Medicaid program, including health information, information collected to determine financial eligibility, etc. The Family Educational Rights and Privacy Act (FERPA) governs the confidentiality of student educational records. Under federal law, information about the identity, diagnosis, treatment maintained in connection with substance abuse training, treatment, rehabilitation, etc., is all protected.

The party responsible for the protected information. The responsible party will vary by the type of data. The designated state Medicaid agency is responsible for protecting Medicaid data. The designated state vocational rehabilitation agency is responsible for protecting federally regulated vocational rehabilitation information. The Department of Corrections is required to protect certain information about persons in its custody, as required by state law.

The required elements of an authorization to disclose protected information. Typically the law creating the protection for information also specifies the conditions under which an individual can authorize the disclosure of his or her information. HIPAA provides the most comprehensive specification of what must be included in an authorization including a description of the information to be disclosed, identification of the person authorized to disclose the information, the identity of a person or class of persons to whom the information may be disclosed, and a description of the purpose for which the information may be disclosed.

The conditions under which protected information can be disclosed without authorization. The ability to disclose without authorization varies with every regulatory scheme. For example, under federal law, protected information about substance abuse treatment, etc., can be disclosed without authorization only by medical personnel to meet a bona fide emergency, or to qualified personnel for the purpose of conducting scientific research, audits, or program evaluation. By contrast, the Department of Corrections can release to any state agency information about any person receiving services from DOC, if the disclosure is necessary to carry out the statutory function of the agency. HIPAA identifies certain conditions where disclosure is permitted with individual authorization. Two government programs serving the same or similar population groups can share information if necessary to coordinate the covered functions of the programs or improve the management of the covered functions.

The requirements for “de-identifying” information so that protections are no longer needed. HIPAA provides the most comprehensive listing of identifiers that must be removed in order to de-identify information. Other laws, if it addresses de-identification, do not provide the same level of guidance.
Memorandum of Understanding

Two state agencies wishing to share information will need to negotiate a memorandum of understanding (MOU) governing the sharing of information. The MOU will address many of the same elements but the legal hurdles for sharing the information will be different.

*With Authorization.* Sharing information at the operational level typically will be governed by a signed authorization. In negotiating an MOU to share information with an authorization, the party responsible for the data will want to address

- **The type of information to be disclosed.** Programmatic staff will identify the data elements that need to be shared.
- **The identity of the persons or class of person to whom information may be disclosed.** Programmatic staff will identify to whom the information may be disclosed.
- **The permitted uses of the information.** On the operational level, the permitted use of information may be coordination of services.
- **The authorization form.** The authorization form will provide the most significant legal hurdle requiring the approval of all who are agreeing to disclose information. It has to be written to meet programmatic and legal needs and still be sufficiently brief and straightforward so the person asked to sign it knows what he or she is signing.
- **The protocol for recognizing an authorization.** Under the Data Integration project, several alternative strategies were identified for controlling the electronic exchange of information when conditioned on an authorization. One strategy would require the authorization to be electronically “registered” before the exchange of information is permitted. Another strategy would permit a “trusted” end-user (i.e., an end-user approved by the data contributor) to represent that an authorization is on file and, upon appropriate authentication and verification, identifiable information is returned. In both cases, prior authorization is required before information is disclosed. The registered authorization would take longer but would provide better assurance that an appropriate authorization was made; registered authorizations generally have more specific conditions and control requirements. The “trusted” authorization might facilitate quicker and easier service coordination but would rely more on the good faith and security practices of end-users. Governing law will dictate the types of controls on the authorization that would have to be in place.

*Without an Authorization.* Linked, de-identified data is created by linking identifiable information. Once linked, the identifiers can be eliminated and the de-identified information no longer requires protection. For linked data to be useful for analytic purposes, its disclosure cannot be conditioned on an authorization. While HIPAA allows the disclosure of protected health information to create de-identified, aggregate data, other regulatory schema were not written to govern the type of electronic exchange of information. Thus, under some regulations, a state agencies must overcome a significant
legal hurdle – finding the authority to disclose information without authorization – in order to create critically useful de-identified aggregate information.

An MOU governing the disclosure of information without authorization, for the purposes of linking, will have to address the:

- information to be disclosed;
- identity of the persons or person to whom information may be disclosed;
- permitted uses of the information; and
- standards for de-identifying the data.

Because each privacy statute or regulation will have different limitations on when disclosure of information without authorization is permitted, each proposed disclosure for linking will have to be measured against the statutory or regulatory permissions in the statute. Each of the elements, the type of information to be disclosed, the identity of the persons to whom information can be disclosed, and the permitted use of the information all must satisfy the governing laws. Programmatic and legal staff will need to play strong roles in meshing the programmatic needs with legal constraints.

Other Elements of an MOU. Ideally, every MOU would also address the protocols end-users will use for protecting information, as well as training requirements for end-users to make sure that they know what is expected of them. All disclosure of information under any MOU, with or without authorization, will be subject to identical controls to manage, authenticate and track all access.

Data Use Controls

The written MOU will need to be implemented as electronic rules in IDA. Ideally, IDA would absorb the complexity of controlling access by offering certain electronic tools and control. These might include:

- **Electronic data dictionary.** Each data contributor participating in IDA would publish their potentially available data elements through an electronic data dictionary. The data user could access the data dictionary to identify those data elements it wished to access. The data user’s selection would be subject to the approval of the data contributor.

- **Electronic classification of end-users.** A classification system would identify the level and type of access for potential classes of end-users. This classification system would define what data elements could be accessed, for whom, for how long, and under what restrictions. According to the terms of the MOU, the data user state agency could propose a classification of its personnel, subject to the approval of the data contributor. The end-users’ user ID and password would be used to enforce the classification system. End-users could also be identified to the system by their role and physical location.
Potentially, one category of end-user could be the “trusted” end-user, or someone who would be trusted to appropriately secure a paper authorization before accessing the individually identifiable information.

- **Protocol for approving electronic implementation of the MOU.** Before a data user is given access to any data, the data contributor would approve the data user’s proposed electronic implementation of the MOU. The data contributor would have an opportunity to review the data elements and the end-users.

- **Protocol for managing the persistence or “duration” of availability of delivered data under the MOU’s requirements.** As data is made available to the authorized and authenticated end user, the electronic implementation will not only audit access and but will also ensure that the actual information is retained in a secured physical environment that is not in the direct control of the end-user. Data made available does not necessarily imply data delivered. Available data will be destroyed based on the requirements of the MOU.

- **Option for physical retention and control of data made accessible under the MOU.** Technical strategies can be implemented that prevent exporting the data. The data could be encrypted and accessible only on an authorized tool or location; that has been previously installed with appropriate decryption keys. Each service request under the MOU will be managed and encrypted individually.

A number of data use controls cannot be implemented electronically. For example, once accessed by the end-user, there are no electronic controls over how the information is actually used by the end-user. Auditing compliance with the MOU, supported by appropriate electronic tools, will be an important quality control for enforcement of the MOU. These audit compliance practices should be comparable to those currently in place for current paper-based disclosure of confidential information (e.g. case files/notes, faxes and voice recordings). In addition, electronic implementation can facilitate the procedural review and audit process, with the capacity to produce relevant reports, and audit and track access. These electronic tools could be similar to a robust incident tracking, document management, and workflow system.

**Conclusion**

While the State has a vital need for linked and integrated information, it is critical for the State to comply with confidentiality requirements governing protected, personally identifiable information. The process of developing an agreement to share information will involve collaboration between legal and program staff. The complexity of implementing the MOU electronically can be concealed from non-technical staff by building electronic tools that support the exchange of information, while still supporting the enforcement of confidentiality requirements.