NORTHWESTERN
UNIVERSITY

Protocol for Exchange and Shared Responsibility for Institutional Data

Revision 1.0

Table of Contents

Preface

There are many cases where data is shared, particularly between enterprise application systems and Local Management Information Systems (LMIS). This will continue and will be driven by better systems and tools that further enable data sharing.

Once the custodians of the source and requesting systems reach an agreement to share data, it is important to document that instance of data sharing. It may also be important to document a mutual understanding of the particular parameters of a data sharing agreement, including the responsibilities and security needs associated with provisioning data to the requesting system. Such documentation will lend structure to the implementation and maintenance of the data sharing agreement, and will assist in instances of personnel turnover. On the other hand, undocumented or 'handshake' agreements pose risks to the institution, particularly if sensitive or non-public data becomes available to unauthorized individuals or entities because the second system is not appropriately secured and/or is not implementing institutional policies regarding data access.

The purpose of the following example is to illustrate the range of issues to consider in documenting a data sharing agreement. It comprises a full set of recommendations for which the parties to a particular agreement will determine the extent and level of implementation.

Intended Audience and Scope

This document is intended for data stewards and system administrators charged with implementing the transfer of information, particularly from an enterprise computer system to a system managed locally by a department, division, or school. Such transfers are commonly used by

the second computer system to offer enhanced or tailored services to other parties within the University (the "end-users"). This document does not address:

- Processes or criteria for classifying information sensitivity or assessing risk;
- Processes or criteria for determining if a request for access to information is legitimate or whether it will be granted or denied;
- Processes for granting access and provisioning data to end-users;
- Processes or criteria for supplying information to outside business partners, but this may serve as a guide.

This document applies to situations where an agreement to transfer information has been reached and specific requirements are to be enumerated and implemented. The depth and breadth of those requirements are left to informed judgment of the parties; however, many of the suggestions contained herein are recommended to promote shared responsibility for the protection of the University's data, and to ensure compliance.

Background

The administrative functions of the University are reaching an unprecedented level of automation. Virtually every administrative office of the University relies upon a computer-based system to carry out day-to-day activities. Many University records and transactions are wholly electronic and are never printed. As software allows these offices to support virtually "paperless" processes, they will naturally seek to use this institutional data to improve their academic, administrative and research performance.

The University's stores of electronic information are becoming important assets for shaping business and academic activities. Software functions, secure access to data and operation of the network itself can be – and will be – tailored to the immediate attributes of persons (e.g. standing, departmental affiliation, course registration, reporting structure, etc.). Decision-support software can only be useful with access to resource information such as funds available, staff schedules, and space allocations.

Providing access to information sources improves the data management environment in two fundamental ways. First, it establishes an agreed authority for the information – "one version of the truth" that exists and is acknowledged by all as available for authorized purposes. Second, it provides convenient access to information, with shared responsibility for its protection. Without approved means of access to official information, application providers will find workarounds which may introduce more risk.

Division, school, or departmental computer applications (LMIS) should have convenient access to authoritative information; however, the University must educate the information requesters to their responsibility to protect the data to the same degree as the authority (e.g. the data steward or system administrator) and insure that the system that receives data is properly secure. An explicit process for defining access, describing the means for access, acknowledging shared responsibility for data protection, and agreeing to regular reassessment frames and documents the contract – or protocol – for information sharing.

In August 2004, the Data Security – Access Working Group of the Administrative Data Council filed a report and recommendations.[1] That working group advised that:

> The goal of both enterprise and local level information systems is to provide the highest quality data to the users in a timely fashion. As a general policy, in a university

[1] "Data Security – Access: Report to the Administrative Data Council", S. Anderson *et al*, August 2004.

> environment that thrives on academic freedom and the exchange of ideas, access should be restricted to only specific information for very specific statutory, regulatory or policy reasons. To the maximum extent, information elements that do not have specific restrictions should be as widely accessible as possible.

The concepts and processes suggested below are derived from that report and its recommendations.

The Goal – Make Data Available With Shared Responsibility

The process of automating administrative functions has been driven by the uneven application of technology in the marketplace. For example, the use of computers for accounting was mature long before the Internet introduced the concept of Web-based learning. In all higher-education institutions, this has created organizational structures concerned with focused data gathering, data management, quality control, and data protection for only specific functions.

This organizational model has placed just a few persons in roles of responsibility for the quality and security of institutional data. The future business and academic needs of the University must use this information to shape systems and processes. To do that a wider group of computer applications must have *informed* data access and shared responsibility for use of that data. The informed nature of this access is vital because much of the data of interest is sensitive or falls under increasing regulatory protections and must be handled appropriately.

A key component for an effective data management policy is acknowledging shared responsibility between the persons with titular oversight and those who offer services reliant upon access to information. This document describes an approach where oversight is focused on accurate definition and adherence to process, with accompanying shared responsibility and accountability. A formal agreement between the provider and consumer, which includes stipulations for data handling, training, and technical security measures, becomes a protocol for access.

Maintaining the Integrity of Authoritative Data Sources

An important value of using central data in local management information systems is to orient and provide users with consistent core information, particularly about people and organizations. Displaying names, titles, department affiliations, addresses, financial attributes and other expected items can reassure the user and contribute directly to the efficiency of business processes. However, the local system should be consistent in its use of such data items and should not allow the values to be changed in the local system. To do so may deliver the impression that the source data item is being modified and that official University records are thus updated. This assumption is often erroneous, unless the local system is capable and approved to execute that change directly within the authoritative system. If the value of a particular data item is in error, then it should be corrected in the source system and then propagated again to the receiving system.

Several examples illustrate the benefits of maintaining the integrity of official source records:

- A local system which permits users to change their names within it could frustrate a person whose name is misspelled in the authoritative source. Changing it locally will have no effect on directories or other displays of identity taken from the central source.

- A local system which recodes authoritative source information into aggregated categories, or derives values from the values of authoritative data items may unintentionally misrepresent a person's employment or academic standing. For example, "admitted student" is not the same as "student" in some academic processes. Neither is "instructor" the same as "faculty". To the extent the local system must support such derivative values or categories, they should be clearly labeled as derivative. For example, a local system might need to recode or aggregrate a value from an authoritative title such as "Assoc Professor" to "Professor". In such a case, the local application should label the field 'simplified title'.

By contrast, authoritative source information such as transaction data that is obtained for analytical or business process purposes is sometimes intended to be modified locally for modeling and forecasting purposes. Once finalized and approved, such data is then updated within the authoritative source system. Naturally, the local system should take care to label displayed information in a manner that describes it accurately to the user.

Data Exchange Protocols

A data exchange protocol describes the conditions, environment, and methods for enabling information to flow between computer systems. The details of each individual protocol will be negotiated between the data steward and the requesting administrator based upon the sensitivity of the information and overall risk assessment.

The data exchange protocol is an *enabling* construct – it is intended to make information available under reasonable conditions. At the same time, it is also a means to ensure that the sharing is *informed* as to the necessary security, data handling, and data retention steps required. In addition, the protocol is a *contract* between administrators in which they agree to abide by the protocol and to be held responsible for compliance.

Goals for a data exchange protocol

A data exchange protocol should seek to make information more readily available, to inform the users of the information of their responsibilities, and to document the University's established practice for protecting information.

- Document efforts to protect information.
  The protocol should be complete and comprehensive to the point that a reasonable observer would agree that the University is taking appropriate steps to safeguard information from accidental or unauthorized release.
- Inform parties of the sensitivity and intended use of the information.
  The protocol serves to clarify the business driver for the information, and to alert the parties to the protections required.
- Define under what circumstances, if any, the values of data items may be changed
  See "Maintaining the Integrity of Authoritative Data Sources" above.
- Clearly describe the shared responsibilities for information protection.
  The protocol documents that the information will be passed from one administrative realm to another and that responsibility for appropriate use and protection resides in each realm separately. Once passed to the recipient, that party becomes responsible for protecting the information and using the information for the purposes described.

Protocol requirements

To be effective in documenting the University's efforts to adequately protect information, a data exchange protocol should establish expectations in the following areas:

- Safeguards and best-practices as a condition for access.
  There should be clear statement of how information will be housed and guarded from unauthorized access.
- Baseline for technical, security and process certification.
  There should be reasonable and effective requirements of how computer systems are secured, maintained, and certified as compliant to a standard. This will also address data access techniques, frequency of access, needs for encryption, etc.
- Clear requirements for training.
  There should be an explicit program for training staff and end-users that will have access to the information about policy and regulatory requirements for its handling and disclosure.
- Clear definition of shared responsibility and accountability.
  There should be a careful description of what responsibilities administrative staff, maintenance staff, and end-users have individually and collectively for the information and how persons will be held accountable for failure to comply with handling and disclosure policies.
- Expectation of re-certification.
  There should be clear statements about the need to re-certify the use of the information through security audits and staff training.

Recommended Components of a Data Exchange Protocol

The following is a general data exchange protocol template that may be used as a starting point for authorities who will be sources of sensitive or non-public information to other computer systems (once again, this process is focused on computer-to-computer transfer of information).

A given source system department will develop at least one and perhaps two templates which should be posted on a Web site for ready access by potential requestors. There will be one template for requesting access to sensitive information and perhaps a second for requesting access to public information.

Each data exchange protocol template is created once and then used as a data gathering form for all requests received in the future. Request forms and decisions about those requests should be retained and made available to auditors as needed.

Statement of Purpose	What is the service supported by the requested access to central information? Who will be the ultimate beneficiaries?
Parties to the agreement	Which units of the University are agreeing? Who are the representatives and their authority? The information provider may require that agreement be with a particular level or above (e.g. dean versus department)

Duration of the agreement		What is the term of the agreement and when will it be reviewed next?
Description of the receiving system:		
	Software environment	Described by requestor: Operating system, application layer, Web layer, etc.
	Technical description of access method, frequency of access, seasonality of access, encryption, etc.	Described by requestor: What is the requested means to access the information. How frequently will requests be made? Will the pattern of requests vary over the academic calendar? Is encryption required?
Certification of receiving system		
	Authentication and access management controls	Described by requestor and verified by security audit: Is access to the receiving system and its applications suitably controlled?
	Firewall, intrusion detection, and anti-virus controls	Described by requestor and verified by security audit: Is the receiving system suitably isolated from sources of intrusion and managed according to best-practices?
	Software maintenance and patching controls	Described by requestor and verified by security audit: Is the receiving system maintained at a high level of attention to vulnerabilities?
	Physical security controls	Described by requestor and verified by security audit: Is the receiving system physically secure and protected from unauthorized access?
Administrative staff profile		Who maintains and operates the receiving system? What training will be required concerning the data being provided (e.g. its sensitivity, protection, consequences of disclosure, etc.)?
End-user profile		Who are the end-users of the receiving system? Are they a closed, specialist community, a general community (e.g. all students), or the public at large? What training will be required for users concerning the data being provided (e.g. policies on downloading to local computers, laptops, PDAs, access from off-campus, etc.)?
Data items requested, grouped into classes by sensitivity and treatment. For each class:		
	Categorization of data sensitivity, applicable policies and regulations concerning use and disclosure	This will be provided by the source system administrator. This could be included in the database definition documentation.
	Method and frequency of access	Described by requestor.
	Intended use for the data items in this class.	Described by requestor. Will the data items be examined, displayed to a user, and/or retained?

	Retention of data items in this class	Described by requestor. Will the data items be retained in a receiving system database? If so, for how long? If the information is volatile (e.g. e-mail address) how will the receiving system ensure that the information does not become stale?
	Visibility of the data items in this class to administrative staff and the end-users	Described by requestor. Will the data items be visible at any time to an end-user or to an administrator of the service or system?
	Data item names	List of the make up of this class using data item names from database definition documentation.
Recertification schedule		How frequently will the receiving system be reviewed to assure best-practices in keeping with the protocol?

NUIT Should Review Templates

The data exchange protocol template may include both an initial security assessment and a requirement for periodic recertification. Data stewards will rely upon NUIT to provide this service and attest that the security agreements are met and maintained. To ensure that the template defines the requirements accurately, the NUIT Information and Systems Security/Compliance department should approve all data exchange protocol templates before they are put into use.

Using a Data Exchange Protocol

Once reviewed and approved, the data exchange protocol document should be posted on the authority's Web site as the standard requirements for any administrator to request access to information. The process for submission, review, and expected time for decision should also be posted. By posting the protocol and the instructions, administrators are made aware in advance of the expectations that will be placed upon their individual operations.

Requests received should be logged and tracked. Files of electronic and printed correspondence should be retained for future audit.

When negotiations between the parties have reached a suitable point, the authority should engage the NUIT Information and Systems Security/Compliance department to conduct a security and practice review of the requesting unit. The report of that review, its recommendations and any subsequent reviews to assure compliance should be included in the files.

When agreement is reached and the security environment is confirmed, then the authority should implement the access through agreed-upon means. NUIT suggests review of the options as described in the reference material below.

The authority should track all protocol agreements in force and should request NUIT to conduct reexaminations of security and practices periodically as per the scheduled agreed to in the protocol.