DEPARTMENT OF HEALTH AND HUMAN SERVICES
ENTERPRISE PERFORMANCE LIFE CYCLE FRAMEWORK

<OPDIV Logo>

PRACTICES GUIDE

DATA USE AGREEMENT

Issue Date: <mm/dd/yyyy>
Revision Date: <mm/dd/yyyy>

Document Purpose

This Practices Guide is a brief document that provides an overview describing the best practices, activities, attributes, and related templates, tools, information, and key terminology of industry-leading project management practices and their accompanying project management templates.

Background

The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) is a framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles, and industry best practices. The EPLC provides the context for the governance process and describes interdependencies between its project management, investment management, and capital planning components. The EPLC framework establishes an environment in which HHS IT investments and projects consistently achieve successful outcomes that align with Department and Operating Division (OPDIV) goals and objectives.

A Data Use Agreement (DUA) is a legal binding agreement between the OPDIV and an external entity (e.g., contractor, private industry, academic institution, other Federal government agency, or state agency), when an external entity requests the use of personal identifiable data that is covered by a legal authority, such as the Privacy Act of 1974, Economy Act, Government-wide User Charge Authority, Intergovernmental Cooperation Act, “Special Studies” statute, Joint Project Authority, and the Clinger-Cohen Act. The agreement delineates the confidentiality requirements of the relevant legal authority, security safeguards, and the OPDIV’s data use policies and procedures. The DUA serves as both a means of informing data users of these requirements and a means of obtaining their agreement to abide by these requirements. Additionally, the DUA serves as a control mechanism for tracking the location(s) of the OPDIV’s data and the reason for the release of the data. A DUA requires that a System of Records (SOR) be in effect, which allows for the disclosure of the data being used.

Practice Overview

The Department of Health and Human Services (HHS) defines a “record” as any item, collection, or grouping of information about an individual that is maintained by an Agency. A System of Records (SOR) is a grouping of any records under the control of any Agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, including, but not limited to:

- Name
- Education
- Criminal History
- Medical History
- Employment History
- Financial Transactions
- Any identifying number, symbol, or other identifier such as a finger print, voice print, or photograph

Data use occurs when there is a legal authority for Federal and/or State Agencies to share information in identifiable form (IIF).   An agency may enter into a data use agreement with another entity if authorized by law. The agreement must indicate the legal and statutory authority for use of data. There may be multiple data use agreements in any given project. If there are separate promises between the various entities involved, the agreement must be drafted to reflect the relationships.

Practice Best Practices

When a DUA is Required

Agencies establish data use agreements to conduct many government functions, including developing or modernizing systems, expanded collaboration across agencies or populating databases for operational use. A DUA is a legal document that establishes the legal and program authority that governs the conditions, safeguards, and procedures under which Federal Agencies agree to use data that has been previously established through a SOR. Consideration of Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), the Family Educational Rights and Privacy Act (FERPRA), or the Privacy Act require Agencies to establish the DUA such that legal context is established and demonstrates entities have a full understanding of applicable statutes, regulations and traditional practices. The DUA may require:

- Institutional Review Board (IRB) to oversee data use activities, particularly if the data involves personally identifiable information
- Informed consent documents for potential research participants
- Members of joint projects to be trained on safeguards to protect confidential information

The DUA encompasses all IT projects. DUAs must be developed when any data covered by SOR will be exchanged or used across agencies. In addition, DUAs must be developed when matches involve Federal personnel or payroll records. In concurrence with a DUA, a project must also prepare an Inter/Intra-Agency Agreement (IA) when the SOR(s) involved in the comparison are the responsibility of another Federal Agency.

An IA, also known as a reimbursable agreement, is a written compact in which a Federal agency agrees to provide to, purchase from, or exchange with another Federal agency services, supplies or equipment. An IA is the document with which the receiving agency agrees to reimburse the providing agency for the cost of the services, supplies, or equipment. In certain cases, two or more agencies may agree to exchange services, supplies, or equipment without a transfer of funds. Although an IA is usually between two agencies, on occasion, an IA may involve more than two agencies.

All funded IT projects must prepare an IA in order to provide to, purchase from, or exchange with another Federal agency services, supplies, or equipment.

Elements of a DUA

- Name
- Legal Authority for Data Use
- Program Authority for Data Use
- Purpose
- Background
- Mutual Interest of Entities
- Responsibilities of Entities
- Funding Information
- Costs and Reimbursement
- Custodian of Data
- Agency Point of Contact (Project Officer)
- Data Security Procedures
- Inspecting Security Arrangements
- Data Transfer, Media and Methods for the Exchange of Data
- Reporting Requirements
- Records Usage, Duplication, Re-disclosure Restrictions
- Record Keeping, Retention and Disposition of Records
- Potential Work Constraints
- Ownership
- Conditions for Reporting Results and Public Release of Data
- Policy and procedures for releasing data to researchers
- Penalties for Unauthorized Disclosure of Information
- Term of the Agreement
- Constraints, including Performance standards, DUA Review Procedures, Audit Clause, Liability Issues, Definition of a Breach

- Resolution of Conflicts
- Concurrences, including Third Party Concurrence

Timeframe and Completion of the DUA
The HHS Enterprise Performance Life Cycle (EPLC) requires as part of a project's Design Phase that security documents (Certification and Accreditation [C&A], Privacy Impact Assessment [PIA], System of Record Notice [SORN], and Computer Match Agreement [CMA] be reviewed for completeness and accuracy. The Data Use Agreement is conditionally required as part of a project's Design Phase. It is the responsibility of the IT Project Manager to ensure that the System Owner prepares and/or approves the initial DUA. The IT Project Manager and/or System Owner must then submit the DUA to the Office of the Chief Information Security Officer (OCISO) for formal review and clearance of the DUA, and to Institutional Review Boards of the entities involved in the data use agreement.

Practice Activities

For software development projects the following practice activities are appropriate:

- **Identify** – Identify the need for a DUA
- **Document** – Document the fields / systems that will be exchanged
- **Consistency** – Ensure that data-use-agreements are consistent with the contents and format of NHIN CONNECT DURSA agreements
- **Develop Agreement** – Prepare the Inter/Intra-Agency Agreement (agreement between the sending and receiving agency)
- **Review** – Review the DUA for completeness and accuracy
- **Submit** – Submit the DUA to the OCISO and Institutional Review Boards for formal review and clearance