STATE OF MAINE EXECUTIVE BRANCH DATA SHARING AGREEMENT (DSA) GUIDELINES

When implemented effectively and efficiently, data sharing between State of Maine agencies can improve programs and services, leading to better outcomes. The purpose of these guidelines is to achieve consistency among State agencies with regard to how data is shared. Following the best practices outlined herein will promote privacy, security, transparency, and accountability.
Data can be siloed, even within the same agency. These guidelines address what data can be shared and under what conditions, thereby minimizing the risks of exposing personally identifiable information (PII) and protected health information (PHI). This guidance seeks to ensure compliance with relevant data protection regulations and laws (e.g. HIPAA, FERPA, CFR, CJIS, etc.) while strengthening public trust. These guidelines are consistent with MaineIT policies. For more information, please reference the associated white paper.

Notwithstanding anything herein to the contrary, the Data Management and Governance Practice acknowledges separate state, and federal laws may apply to an agency's data. In the event of a conflict between these guidelines and a separately applicable law, agencies are advised to seek legal advice if they have questions.

A sample data sharing agreement has been provided. Agencies can use it, or craft their own in accordance with the guidelines listed below. For guidance on specific legal provisions, please consult your agency's in-house legal counsel or the Office of the Attorney General (OAG).

Scope

DSAs should be used when large data sets or an entire system is being exchanged between entities. For example, a DSA would be appropriate if DHHS and DOE needed to exchange information about immunization status for ALL school-aged children in Maine.

Agencies define terms and conditions related to the data being shared. In the scenario above, either DOE or DHHS may elect to provide only de-identified or aggregated data, rather than individual records with PHI/PII. Conversely, they could elect to share raw data and would need to ensure compliance with FERPA and HIPAA, respectively. A DSA would help these agencies comply with a legislative mandate (and reporting requirements) by providing structure and consistency that may not otherwise be prescribed in the legislation itself.

A Data Sharing Agreement (DSA) is neither necessary nor recommended for instanced transmission of PHI/PII. These situations should be addressed through individual Authorization to Release Information forms or similar waivers. An example of instanced data sharing is when immunization records are provided to a school for a child in foster care.

Data Sharing Checklist

A multi-party Data Sharing Agreement should include the following components:

Parties and Effective Dates	Identify sending and receiving parties, and effective dates (duration) of the DSA
Purpose	Clearly identify the reason for data sharing
Access to Data	Outline the criteria and restrictions for accessing data, and identify authorized users
Data Exchange	Specify whether the data exchange is ad hoc or standing
Data Transmission Terms & Conditions	Detail the criteria for transmitting, storing, and maintaining data to ensure compliance with laws and regulations
Reliance	Describe the transmitting parties' reliance on the receiving party to adhere to the DSA terms
Data Breach or Security Incident	Detail the protocol for notifying involved parties of a data breach or security incident, with an emphasis on immediate communication
Data Disposal	Provide instructions for the receiving party on the acceptable disposal of data received via the DSA
Enforcement	Outline each party's responsibility to adhere to the data sharing guidelines within their organization's policies
Jurisdiction and General Provisions	Include specific terms, requirements, provisions, and information relevant to the parties and their respective regulatory environments.
Termination of Agreement	State that the agreement is effective upon signature and remains valid until its purpose is fulfilled, the end date is reached, or relevant laws change. Allow for early termination, requiring written notification 30 calendar days prior. If there are concerns about misuse of data or intentional unauthorized disclosures, please consult with the Office of the Attorney General to determine if immediate termination is appropriate.
Authorized Representatives(s)	Identify the authorized signatories on behalf of agencies

1. **Parties and Effective Dates:**

   In this section, the sending and receiving entities are identified, as well as the effective dates (duration) of the DSA. We recommend creating DSAs for one year and reviewing them for renewal, if appropriate. DSAs can be created on a standing (permanent) basis. If agencies choose to create standing DSAs, they should maintain an inventory to allow for periodic review. More information is provided below, in the "Types of Data Exchange" section.

2. **Purpose:**

   In this section, both organizations should state in non-technical language the purpose(s) for which they are entering into the agreement. For example, "Data will be shared between DHHS-CDC and DOC to facilitate tracing and testing of tuberculosis in State facilities."

3. **Access to Data:**

   The purpose of this section is to outline the criteria and restrictions for access to data, specifying how data should be released, used, and safeguarded by authorized users to ensure compliance with relevant laws and regulations.

4. **Data Exchange:**

   This section identifies whether the parties will be entering into a limited (ad-hoc) or permanent (standing) data sharing agreement. For further details, please consult the Data Sharing Agreement Guidelines Whitepaper .

   - Ad-hoc exchanges are temporary and created on a one-time basis for emergency response or specific needs, such as a singular report.
   - Standing exchanges are routine data exchanges to support ongoing programs, services, or business processes.

5. **Data Transmission Terms and Conditions:**

   This section outlines the criteria for transmitting, storing, and maintaining data to ensure compliance with laws and regulations. Please refer to the following best practices and standards from the Data Exchange Policy.

   MaineIT is responsible for ensuring end-point security and file transfer protocols between agencies and if data is shared with an external entity, these requirements still apply for SOM transmitted data.

6. **Reliance:**

   This section describes the Transmitting parties' reliance on the Receiving party to faithfully adhere to the terms of the DSA.

7. **Data Breach or Security Incident:**

   The purpose of this section is to outline the protocol for notifying involved parties of a data breach or security incident, emphasizing immediate communication within 24 hours of discovery, and providing follow-up information as soon as it becomes available.

8. **Data Disposal:**

   This section provides instructions for the receiving party, regarding acceptable disposal of data received via the DSA.

9. **Enforcement:**

   This section outlines each party's responsibility to follow the data sharing guidelines.

   Each Party's data leaders shall ensure compliance with the items stated in this agreement within their organization's policies, procedures and regulatory environment.

10. **Jurisdiction and General Provisions:**

    This section allows agencies to include their department or agency specific terms, requirements, and information below. This may reflect the regulatory environment alluded to in the ""Enforcement" section above.

11. **Termination of Agreement:**

    The Termination of Agreement section outlines that the agreement becomes effective upon signature and remains valid until its purpose is completed, the end date is reached, or relevant laws change. Any party can withdraw by providing thirty days' written notice. If there are concerns about misuse of data or intentional disclosures, please consult with the Office of the Attorney General to determine if immediate termination is appropriate.

12. **Authorized Representative(s):**

    This section identifies the authorized signatories on behalf of agencies. Information should include the signatories' name, title, and date signed. Fields can be added for this information for original (wet) signatures. Virtual signatures automatically include date and time of signature.