Published on *University of Colorado* (https://www.cu.edu)

Data Management Group Process [1]

Data Management Groups manage multi-campus access and use of data here at CU

A Data Management Group (DMG) for each business domain is typically composed of data stewards and data custodians and/or their designees. These individuals shall be appointed by and accountable to the data trustees for the related business domain. The DMGs are part of the data governance program established by the Data Governance policy, APS 6010 [2], to ensure that data is managed as a material asset, data provides value, meets compliance requirements, and risks are managed appropriately. Projects involving single-campus data should contact the appropriate data trustee [3] to request approval for the use of that data on their campus.

DMG Process

Decisions about new uses of multi-campus data are made by the corresponding Data Management Groups (DMG). There are three multi-campus DMGs: student, employee and finance. The data management groups are composed of the data stewards (the delegates of the data trustees) from each campus and representatives from IT groups to assist with questions. Decisions are made by the data stewards or data trustees. Each of these groups typically meets on a monthly basis to discuss multi-campus data issues. In the event of a more urgent need for discussion, the groups may choose to discuss via email or call an out of cycle meeting. Because each DMG group only meets monthly, please plan ahead in your projects and come well prepared to avoid a need for a second meeting. If you have any questions about preparing for a DMG meeting, contact data.governance@cu.edu [4].

If a project involves a new use of multicampus data or a system or process change that will impact multiple campuses, then requestors should complete a data governance request form and submit the competed form to data.governance@cu.edu [4]. It will be reviewed by the Office of Information Security, who may reach out for more details or clarification. After review, OIS will forward the request to the appropriate data management group for discussion in their next meeting. The organizer of the DMG meeting will contact the requestor to invite them to the DMG meeting where they can answer any questions from the data stewards or data trustees.

DMG Responsibilities

- Developing and managing processes to ensure confidentiality, integrity, availability and usefulness of data (see next section)
- Managing risk to data including escalating identified significant risk to data owners and advising data trustees on risk acceptance decisions

- Defining access, quality and usage guidelines for data
- Reviewing and managing requests for access to data
- Educating and sharing best practices with respective campus and system stakeholders
- Managing data quality processes
- Constructing business access that dictates security procedures and rules for third-party usage of system data

DMG Evaluation Considerations

- Authority and purpose for data collection including:
    - determine the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy
    - provide adequate notification of the purpose(s) for which PII is collected
- Accountability, audit, and risk management of data to ensure effective controls for governance, monitoring, and mitigation to demonstrate that units are complying with applicable privacy protection requirements and minimizing overall privacy risk.
- Data quality and integrity processes to ensure that highly critical data is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices and in support of the university strategic objectives.
- Data minimization and retention processes so that the university collects, uses, and retains only personally identifiable information (PII) that is relevant and necessary for the purpose for which it was originally collected.
- Individual participation and redress processes so that individuals are active participants in the decision-making process regarding the collection and use of their personally identifiable information thus enhancing public confidence.
- Transparency by providing public notice of information practices and the privacy impact of programs and activities.
- Guidelines and processes to ensure that use of personally identifiable information (PII) is limited either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law.

Visit Data Management Group Members [5] for current membership.

Groups audience:
Office of Information Security
Right Sidebar:
DMG Request

Links
[1] https://www.cu.edu/security/data-management-group-process
[2] https://www.cu.edu/ope/aps/6010
[3] https://www.cu.edu/node/242344/edit
[4] mailto:data.governance@cu.edu
[5] https://www.cu.edu/security/data-management-group-members