Data Analytic Core
Privacy Policies

Security

1 Inventory of PII/PHI

The DAC:

a. Establishes, maintains, and updates annually, an inventory of all directories in the DAC Information System containing instances of PHI/PII. This inventory is maintained by the DAC Compliance Coordinator and is updated more often based on the approval of new Data Use Agreements and then a DUA is closed.
b. The DAC Director, Senior Privacy Officer for DAC Information Systems, and the Dartmouth College CISO review updates of the DAC Information System PHI/PII inventory no less than annually.

2 Privacy Incident Response

The DAC:

a. Develops a Privacy Incident and Breach Response Plan that is aligned with the DAC Security Incident and Breach Response Plan.
b. Provides an organized and effective response to privacy incidents and breaches in accordance with HHS and CMS Privacy Incident Response Plans.

For any incident involving CMS data, the DAC Director is responsible for **notifying CMS within one (1) hour** of any suspected incidents wherein the security and privacy of the CMS data may have been compromised.

The DAC monitors the use of information systems to determine if any DAC users have violated policies and procedures. In the event of a suspected violation of data use or breach, the DAC Director, in collaboration with the Dartmouth Chief Information Security Officer, will investigate the potential violation or breach to determine the extent, severity, and nature of the event.

1. Notify the appropriate personnel when a violation occurs and determine the severity and willfulness of the violation.
2. Determine the appropriate disciplinary action for the violation, including termination of access to information systems, if appropriate.
3. Determine if criminal or civil prosecution is warranted based on the severity and willfulness of the violation.