Procedure For Storing Files Containing Personal Identity Information

Scope

This procedure defines the allowed storage locations to store files that contain Personal Identity Information at Georgia College.

For purposes of this procedure, we use the USG Standard 5.7.2, Defining Personal Information, which aligns with the Georgia Personal Identity Protection Act:

Personal information is information that identifies or describes an entity by name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: name, address, telephone number, Social Security number (SSN), date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer Internet Protocol address or routing code and credit card number or other credit card information. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal information includes, but is not limited to:

- Protected Health Information (PHI) - individually identifiable health information created, transmitted, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers who are conducting electronic transactions to ensure the privacy and security of electronically protected health information from unauthorized use, access, or disclosure.

- Personally Identifiable Information (PII) - any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, a visitor to the U.S., or employee or contractor to the institution. Some PII is not sensitive, such as the PII on a business card. Other PII is considered Sensitive Personally Identifiable Information (Sensitive PII) and if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Procedure

Electronic records (aka. files) containing PII or PHI must be encrypted when stored on any electronic device (computer or mobile device). We use AxCrypt at GCSU to encrypt files.

Files that are transmitted electronically must use a secured (user name and password) and encrypted transmission.

Electronic records which contain PII or PHI may be stored on local hard drives (on GCSU issued systems), but only on fully encrypted hard drives. Files with PII or PHI should never be stored on systems that are not issued by GCSU.

Storage of electronic records which contain PII or PHI is not approved for use with non-GCSU personal accounts in any system whatsoever.

Files on shared storage:

The defined data custodian must approve electronic records containing PII or PHI that need to be shared with GC employees (ala. department).

Electronic records may be stored on GCSU supplied GC Share drives. Files that contain PII or PHI must be encrypted. The password used to encrypt the files can be shared with the employees who have access to the share.

GCSU employees can use the GCSU approved OneDrive, Teams, or Sharepoint applications that are associated with their GCSU email account. Files and folders in OneDrive/Teams/Sharepoint should only be shared with approved GCSU employees.

Access to these folders (whether on GC Share, OneDrive, or Teams/Sharepoint) should be reviewed by the data custodian every 6 months and the results shared with the data steward.