1.08.04.00 Personally Identifiable Information (PII) (formerly G-053)

Policy/Guideline Area

Governance, Organization, and General Policies

Applicable Divisions

TCATs, Community Colleges, System Office, Board Members

Purpose

TBR institutions create, collect, maintain, use, and transmit personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. TBR institutions are committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations.

Definitions

- Data Custodians - Data Custodians are the people responsible for oversight of personally-identifiable information in their respective areas of institutional operations.
- The Data Custodian (also called a Data Steward or Data Owner) is the person who has administrative control and has been officially designated as accountable for a specific information asset or dataset. This person would determine who has access to what and IT implements the controls to match.
- Minimum Necessary - Minimum Necessary is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.
- Personally Identifiable Information (PII) - Information that has not been lawfully made publicly available and which can be used to distinguish or trace an individual's identity, such as Social Security number driver license, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific

individual, such as date and place of birth, mother's maiden name, etc. Certain privacy laws, and policies based on those laws, may use a different definition of PII.

- Directory information - Directory information is information that is generally not considered harmful or an invasion of privacy if released. It can also be disclosed to outside organizations.

Policy/Guideline

I. Policy

A. Members of the TBR community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it.

B. All individuals who dispense, receive, and store PII have responsibilities to safeguard it.

C. In adopting this policy, the System is guided by the following objectives:

1. To enhance individual privacy for members of the TBR community through the secure handling of PII.
2. To ensure that all members of the TBR community understand their obligations and individual responsibilities under this policy by providing appropriate training that shall permit the TBR community to comply with both the letter and the spirit of all applicable privacy legislation. Each member institution will be responsible for determining the means of training for its institution.
3. To increase security and management of Social Security numbers (SSNs) by:
    a. Instilling broad awareness of the confidential nature of the SSNs;
    b. Establishing a consistent policy about the use of SSNs throughout the System; and
    c. Ensuring that access to SSNs for the purpose of conducting TBR business is granted only to the extent necessary to accomplish a given task or purpose.
    d. To reduce reliance on the SSN for identification purposes as much as possible.

4. To comply with all Payment Card Industry (PCI) standards.
5. To comply with any other applicable and required standards, regulations and/or laws.
6. To comply with Family Educational Rights and Privacy Act of 1974 (FERPA).

D. Data Custodians are responsible for oversight of personally identifiable information in their respective areas of institutional operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant institutional officials.

II. Scope

A. This policy applies to all members of the TBR community, including all full- and part-time employees, faculty, students, and other individuals such as volunteers, contractors, consultants, other agents of the institution or whose work gives them custodial responsibilities for PII.

III. Policy Requirements

A. Data Custodians

1. Officials responsible for each of the following areas shall be considered Data Custodians:
    a. Student Records
    b. Financial Aid Records
    c. Alumni and Donor Records
    d. Employee Records
    e. Purchasing and Contracts
    f. Research Subjects
    g. Public Safety or Campus Police

IV. Personally Identifiable Information

A. PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official TBR duties, subject to the requirements:

1. That the PII released is narrowly tailored to a specific operational or business requirement;
2. That the information is kept secure and used only for the specific operational purposes for which authorization was obtained; and
3. That the PII is not further disclosed or provided to others without proper authorization.

B. PII may be provided to and handled by third parties, including cloud service providers, with the strict requirement that the information be kept secure and used only for a specific purposes set out in the contract authorizing use of the information.

C. Exceptions to this policy may be made only upon specific requests approved by the institutional official responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and operational needs of the institution.

1. Exceptions must be documented, retained securely, and reviewed periodically by the appropriate institutional official or his/her designee.
2. Exceptions may be modified or eliminated based on this review and shall be documented and retained for auditing purposes.

D. Directory Information, as defined by Federal and State law and institutional policy, will be published following the guidelines defined by the specific law.

E. Colleges may share information covered by FERPA only as permitted by FERPA and applicable policy. Colleges must notify students annually of their rights under FERPA.

F. Information that has been collected that conforms to the HIPAA standards of de-identification or anonymization is not PII.

V. Government-Issued Personal Identifiers

A. Social Security Number

1. Provision of Information

a. TBR institutions collect SSNs:

(1) When required to do so by law;

(2) When no other identifier serves the business purpose; and

(3) When an individual volunteers the SSN as a means of locating or confirming personal records.

b. In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.

2. Release of SSNs

a. SSNs will be released to persons or entities outside the institution only:

(1) As required by law;

(2) When permission is granted by the individual;

(3) When the external entity is acting as the institution's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or

(4) When the Office of General Counsel has approved the release.

3. Use, Display, Storage, Retention, and Disposal

a. SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a TBR official for a TBR operational purpose.

b. The release or posting of personal information, such as grades or occupational listings, keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access.

c. SSNs will be transmitted electronically only for operational purposes approved by the institutional officials responsible for SSN oversight and only through secure mechanisms.

d. The Data Custodians who are responsible for SSNs will oversee the establishment of procedures for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.

B. Non-SSN Government-Issued Identifiers

1. In the course of business operations, TBR institutions have access to, collect, and use non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers, Employee Identification Numbers (EIN), and military identification cards, among others.
2. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard these identifiers.

VI. Other Externally-Assigned Identifiers and Other Personally Identifiable Information

A. TBR institutions shall follow the Minimum Necessary standard and strive to safeguard any externally assigned identifiers which may be collected.

VII. Responsibility for Maintenance and Access Control

A. Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.

B. Access to electronic and physical repositories containing PII shall be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.

C. Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority.

D. All paper documents with PII must be under lock and key or otherwise securely stored.

E. Document retention policies dictate schedules for PII deletion and/or destruction. Proper disposal of PII shall involve cross-cut shredders (for paper), securely wiping/deleting data (for digital information) and other information security approved methods of eliminating this data.

VIII. Enforcement

A. Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of PII may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the institution or, in the case of students, suspension or expulsion from the institution.

Sources

Authority

T.C.A. § 49-8-203

History

NEW Guideline approved August 19, 2014, President's Meeting; effective September 26, 2014. Revised and changed to policy at Special Called Meeting May 14, 2019; Revisions approved September 20, 2024, Board Meeting.