



Health Care Finance & Administration Policy Manual

Policy Number: PRIV 16-013
Policy Subject: Privacy, Security and Confidentiality Training
Approved by: <i>[Signature]</i> Date: 6/3/16

PURPOSE OF POLICY

This policy addresses how Health Care Finance and Administration (HCFA) provides for training of workforce members in the proper use and safeguarding of various types of information, including federal tax return information (FTI), Social Security Administration provided information (SSA information), protected health information (PHI) and personally identifiable information (PII) of benefit applicants and enrollees.

POLICY

HCFA shall provide appropriate new hire and annual training to all members of its workforce on its policies and procedures related to the privacy, security and confidentiality of information created, maintained, used received or transmitted regarding its benefit population. Additionally, HCFA shall provide specialized training as needed to members of the workforce based on their access to sensitive information.

DISCUSSION & LEGAL BASIS

Federal and state laws and regulations require that workforce members who have access to confidential information must be trained on, be aware of, and understand the requirements for protecting the privacy, security, and confidentiality of the information or data. The workforce shall receive the appropriate training, which may include new employee, annual, insider threat, and specialized role-based training, by required compliance dates.

New hires are required to complete New Employee Orientation, which includes an abbreviated

privacy, security, and confidentiality (PSC) training section, and the HCFA PSC in-person training within a reasonable period of time after joining HCFA, but within no more than two (2) quarters of hire date, beginning with the closest end-of- quarter date.

HCFA shall document that all workforce members who must access, use or disclose PII, PHI, FTI, SSA information or any other confidential information as part of their job duties have received appropriate training in compliance with applicable laws.

The HCFA Privacy Office shall periodically review and revise all training materials to ensure the information presented is in compliance with current federal and state privacy, security and confidentiality laws and regulations.

PROCEDURE

- HCFA's PSC training program consists of in-person new hire, and in-person or web-based annual training, and, as appropriate, additional role-based training geared toward the job functions of the employee.
- Newly hired HCFA employees shall receive an email invitation to attend the New Hire PSC Training. All HCFA employees shall receive an email invitation to complete Annual PSC Training. In addition, contractors who may access, use or disclose PII, PHI, FTI or SSA information on behalf of HCFA may be required to participate in the New Hire, Annual PSC Training, and/or any additional role-based training at HCFA's request and discretion.
- To ensure proper documentation, HCFA shall document the attendance and completion of training.
 - For any in-person training:
 - i. An employee or contractor shall be required to fill out a sign-in sheet to verify attendance at the training;
 - ii. Optional evaluation may be submitted upon completion of the training session;
 - iii. An employee or contractor shall be required to submit a Statement of Understanding counter-signed by his/her supervisor; and,
 - For any web-based training:
 - i. The HCFA Privacy Office shall use built-in tracking tools as available to track progress and completion of training for each workforce member.
- The HCFA Privacy Office shall maintain a training database signifying the workforce

member's satisfactory attendance and completion of each required stage of PSC training. Training records shall be retained for a minimum period of five years.

- Upon notification by a workforce member's supervisor, and in consultation with HCFA Human Resources, the HCFA Privacy Office shall schedule the workforce member for the necessary PSC training as job duties require or are affected by a material change in the job plan or as otherwise determined necessary or appropriate. The System Security Office will be consulted where appropriate.
- Failure to attend three (3) consecutive training sessions that have been rescheduled shall be grounds for referral to the Director of Personnel for appropriate sanctions.

DEFINITIONS

Enrollee: An individual currently enrolled in any category of State of Tennessee's Medicaid program (TennCare) and Children's Health Insurance Program (CHIP, known as CoverKids in Tennessee) or in any Tennessee federal Medicaid waiver program pursuant to Sections 1115 or 1915 of the Social Security Act; and, for purposes of HCFA privacy policies, the term may also be used to reference an individual who was previously an enrollee during a period for which there is a privacy request or compliance inquiry.

Federal tax information (FTI) and return information: FTI is any return or return information received by HCFA from the Internal Revenue Service (IRS) or secondary source, such as Social Security Administration. FTI includes any information created by HCFA that is derived from return or return information. A return is any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the Internal Revenue Code and filed with the IRS by, on behalf of, or with respect to any person or entity. Return information, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the Internal Revenue Code.

Health Information: Any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

HIPAA: Health Insurance Portability and Accountability Act of 1996 and for which administrative simplification, privacy, and security regulations are codified at 45 Code of Federal Regulations, Parts 160-164.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

The Privacy Act of 1974: A United States federal law, enacted December 31, 1974, and codified at 5 U.S.C. 552a which establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information.

Protected Health Information (PHI): Information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium, including demographic information that identifies or may be used to identify an individual and that:

- (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (2) Relates to the physical or mental health or condition of an individual.

Workforce Members: HCFA employees, contractors, and vendors, including off-site workforce personnel who have access to HCFA data, except to the extent a workforce member is employed by an agency of the State of Tennessee-other than HCFA -that has implemented its own PSC training policy.

OFFICE OF PRIMARY RESPONSIBILITY

HCFA Privacy and Public Records Office, Office of General Counsel

RELATED FORMS

PRIV 16-013
Rev: 05/2016

Statement of Understanding
Training Sign-in Sheets

REFERENCES:

5 U.S.C. 552a

42 C.F.R. § 431.305

45 C.F.R. § 164.308(a)(5)(i)

26 USCA § 6103(P)(4)(D)

IRS Publication 1075