COSMOS
Navigate the Compliance Universe

HCCA Compliance 101, 4th Edition
APPENDIX I | Sample HIPAA-PHI Procedure

Confidentiality of Protected Health Information

Purpose

To establish a mechanism to protect the confidentiality of individually identifiable patient health and financial information from any unauthorized intentional or unintentional use or disclosure in accordance with the requirements in the HIPAA Privacy Rule (See 45 CFR 164.530).

Procedure

A. "Individually Identifiable Information"—Protected Health Information ("PHI") may not be disclosed or released without a complete and valid written authorization signed by the patient, parent, or legally authorized representative, unless 1) the use of such PHI is for purposes of treatment, payment or healthcare operations, generally, or 2) release of the PHI is specifically allowed by State or Federal law without a valid authorization.

The HIPAA Privacy Rule specifies the following pieces of "Individually Identifiable Information" information that, when linked with health or medical information, constitute PHI (45 CFR 164.514):

1. Names of the individual, and relatives, employers or household members of the individual;
2. Geographic identifiers of the individual, including subdivisions smaller than a state, street addresses, city, county and precinct;
3. Zip code at any level less than the initial three digits; except if the initial 3 digits cover a geographical area of 20,000 or less people, then zip code is considered an identifier;
4. All elements of dates, except year, or dates directly related to an individual including birth date, admission date, discharge date, date of death and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
5. Telephone numbers;
6. ax numbers;
7. Electronic mail addresses;
8. Social security numbers;
9. Medical record numbers;
10. Health plan beneficiary numbers;
11. Account numbers;

12. Certificate/license numbers;
13. Vehicle identifiers and serial numbers, including license plate numbers;
14. Device identifiers and serial numbers;
15. Web Universal Resource Locators (URLs);
16. Internet Protocol (IP) address numbers;
17. Biometric identifiers, including finger and voice prints;
18. Full-face photographic images and any comparable images; and
19. Any other unique identifying number, characteristic, or code;

B. "Patient"—A patient is any individual who seeks and/or receives services within the (organization name) Health System.

C. "Protected Health Information" ("PHI")-Any individually identifiable health or financial information, whether verbal, written, electronic, or otherwise recorded in any form or medium that:

1. is created or received by (organization name) or one of its affiliated entities or one of their employees, agents, or assigns, 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.

D. Health System, its affiliated entities, and their officers, employees, and agents are expected to treat all PHI in any form (paper, electronic, verbal, etc.) as confidential in accordance with government regulations, professional ethics, legal requirements, and accreditation standards, and they:

1. will not divulge PHI unless the patient, parent, or legally authorized representative has properly authorized the release or the release is otherwise required or permitted by law and in accordance with our policies.
2. will release only the reasonable minimum amount of information required by the requestor when a release is appropriately authorized.
3. will take appropriate steps to prevent unauthorized re-disclosures of PHI received from sources other than records.

E. Confidentiality Statement. All employees are required to sign a confidentiality statement before they are granted access to PHI.

F. Training. All employees are required to be trained on policies and procedures regarding confidentiality and PHI to the extent necessary for each individual member to carry out their assigned functions within. This training must be documented and retained with the employee's personnel file.

At a minimum, training will occur:

1. upon hire, or as quickly after hire as feasible, and

2. when an employee's functions or assignment of duties are changed; and/or
3. changes in government regulation or policies and procedures occur.

G. Sanctions. Significant unauthorized or improper release of PHI by an employee or agent may result in disciplinary action up to and including termination of employment (by organization name), civil fines and/or penalties, and/or criminal sanctions (by the government), lawsuits and judgments against the employee. Such conduct by an employee or agent may also result in civil and/or criminal fines and/or penalties against (organization name) or one of its affiliated entities (See 45 CFR 164.530 e(1) & (2)).

H. Reporting. Any employee who believes he/she has observed a violation of this policy should report it to his/her immediate supervisor, the next level of management, any other manager within (organization name) or to the HIPAA Privacy Officer at ###-###-####. An employee may also report a violation anonymously or confidentially to the Compliance AlertLine at 1-888-###-####. Calls received on this line will be referred to the Compliance Department for investigation. There will be no retaliation taken against any employee for making such a report in good faith.