



Office of the Commissioner

Health Information Privacy and Security - Minimum Necessary Policy

Policy#: DHHS-03-13

Issue Date: 7/17/13

Revised Date: 10/01/2019

1. SUBJECT

Health Information Privacy and Security - Minimum Necessary Policy

11.POLICY STATEMENT

The Department of Health and Human Services (the Department) and its offices, programs and facilities will make reasonable efforts to use and disclose only the minimum necessary protected health information (PHI), or other consumer-identifiable information (together, "Protected Information" or PI) in any format to accomplish the intended work-related purpose(s).

111.RATIONALE

The minimum necessary policy is required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and good business practice. Since the Department is also subject to other federal and state legal requirements that require the protection of PI, the minimum necessary policy applies to the entire Department, and all programs, facilities, and offices that create, maintain, access, transmit or receive PI.

IV. PROCEDURE STATEMENT

1. Our workforce will not use or disclose more than the PI necessary to accomplish the intended purpose of such use or disclosure.
2. The minimum necessary policy does not apply in the following situations:
 - Disclosures to or requests by a health care provider for treatment purposes.
 - Disclosures to the individual who is the subject of the information.
 - Uses or disclosures made pursuant to an individual's authorization.
 - Uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.
 - Disclosures to the U.S. Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
 - Uses or disclosures that are required by other law.
 - Where an entire record is disclosed, the reason for such disclosure should be noted.
 - In the event that more than the minimum necessary PI is disclosed, even where the disclosure is inadvertent or unintentional, that disclosure is required by law to be reported to the applicable Privacy/Security Liaison and, in collaboration with the Director of Healthcare Privacy, investigated for potential breach notification under federal and state law.

3. The right to access PI in any format, including on computer systems, must be documented and maintained by the Office Director or his/her designee, in collaboration with the Office of Information Technology, which grants electronic access at the direction of the Department. Such documentation must identify the persons or classes of persons within the Department who need access to PI to carry out their job duties, the categories or types of PI needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit a category (i.e. providers) including doctors, nurses, or others involved in treatment, to have access to the entire medical record, as needed.
4. Routine disclosures must always be limited to the minimum amount necessary to accomplish the purpose of the disclosure, and to no more than the specific PI requested. Standard protocols for repeated requests must be developed and utilized. Criteria must be established and used to ensure that no more than the minimum necessary PI is disclosed in responding to non-routine requests.
5. Reasonable Reliance - the Department is permitted, but not required, to reasonably rely on the judgment of the party requesting the disclosure as to the minimum amount of PI that is needed in certain circumstances. This reliance is permitted when the request is made by:
 - A public official or agency who states that the PHI requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).
 - Another covered entity.
 - A professional who is a workforce member or business associate of the covered entity holding the PI and who states that the PI requested is the minimum necessary for the stated purpose.
 - A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board, after consultation with the Director of Healthcare Privacy and Human Protections Administrator.
6. Intentional failure to follow this policy will result in sanctions, up to and including termination of employment, as set forth in our Health Information Privacy and Security Sanctions Policy.

V. DEFINITION

Protected Health Information is information about an individual, including demographic information, that may identify the individual, which relates to the individual's past, present, or future physical or mental health condition, related health care services or payment for such services.

VI. DISTRIBUTION

All Staff via e-mail and posting on the Department Intranet.

Date

5/8/17



 Mary C. Mayhew
 Commissioner