Individual's Rights to Access and Copy PHI

Reference#: 06-06	Category: PHI Data
Policy Owner: Compliance Committee	Approved By: Compliance Committee
Effective Date: 10/1/19	Revision Date: 12/24/2018

Policy Statement: Patients have the right to access and copy their own protected health information (PHI) maintained/retained by the organization, including any business associates on behalf of the organization, in the Designated Record Set (DRS).

General Scope of Policy: This policy applies to Women's Health USA (WHUSA) and Women's Health CT (WHC), the Management Services Organization (MSO), its participating physicians, clinicians, employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of WHUSA and have been designated as part of the WHUSA HIPAA Health Care Component.

Definition: The Designated Record Set (DRS) is:

1. A group of records maintained by Women's Health USA that are:
    a. Medical records and billing records about an individual maintained by or for Women's Health USA
    b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for Women's Health USA; or
    c. Used by or for WHUSA to make decisions about an individual
2. The term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for Women's Health USA.
3. Note that the DRS may include information that has been received from another provider; such information must be included when granting access to records by individuals.
4. Reference WHUSA's "HIPAA Terms Glossary."

Policy Objective: To establish policies and procedures for allowing a patient access, inspect, and copy his/her Protected Health Information (PHI) in accordance with HIPAA compliance rules and regulations.

Exceptions: Individuals may be denied access to:

1. Psychotherapy notes,
2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceedings, and
3. Information provided in confidence that, if provided to the individual, would reveal the source of the information.

Procedure:

Individual Rights:

1. An individual generally has a right to access and copy his/her PHI maintained in the DRS, including that provided by another healthcare provider.

2. Individuals have the right to obtain electronic copies of PHI in the DRS that is maintained electronically.

Minors and Parental Rights

3. WHUSA may allow a parent access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law. There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are:
    a. When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law;
    b. When the minor obtains care at the direction of a court or a person appointed by the court;
    c. When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship; and
    d. When legal custody has been granted to a specific parent, the person who has such custody is the one who must authorize or consent to treatment of the minor.

Written Requests:

4. A written request for inspection and copying of PHI must be submitted to the HIPAA Privacy Officer/Compliance Officer.

Time to Respond to Written Requests:

5. Responses to requests for access to protected health information under this policy (by either granting or denying the request) must occur within thirty (30) days after the request is received.
6. If an extension is required, the individual should be notified of such request and in no case, should an extension exceed thirty (30) days.
7. The HIPAA Privacy Officer/Compliance Officer or their designee should follow up on a patient's request if necessary, to clarify what information the person is seeking to access. The HIPAA Privacy Officer/Compliance Officer or their designee should record on the request form the results of the discussion and initial or sign his or her notes.

Denial of Access:

8. If the request is denied for an individual to access requested records, a written notice must be provided to the individual indicating such denial and the reason(s) for the denial.

Service Fees:

9. Postage and labor charge(s) may be assessed for copying and mailing services. These charges will be based on the Fee Schedule and may not exceed the incremental costs of providing access.

Denial of Access Without Rights of Review:

10. In addition to the circumstances identified in the Exceptions above, denial of access without a right of review may occur:
    a. Where information was compiled in anticipation of litigation.
    b. Where care was provided under the direction of a correctional institution and provision of access would jeopardize health, safety, or rehabilitation.

c. Where information was collected in the course of research that includes treatment of the individual and the individual agreed to a suspension of the right of access during the research period.

Denial in Accordance with Other Applicable Law:

11. Access may also be denied in accordance with the applicable law.

Denial of Access With Rights of Review:

12. Denial of access with a right of review may occur:
    a. Where access is determined by a licensed professional to be likely to endanger the life or safety of the individual or another person.
    b. Where access is required by the individual's representative and a licensed professional determines that such access is reasonably likely to cause substantial harm.

Individuals Rights to Review by Other Licensed Professional:

13. If the basis for denial of access gives the individual a right to review, the individual has the right to have the denial reviewed by a licensed professional who did not participate in the original denial decision. Such review will be completed within thirty (30) days of such request. WHUSA will provide the individuals with a notice of the reviewer's decision and will comply with the determination to either provide the requested information or deny access to such requested information.

Timeframe to Act on Requested Access:

14. WHUSA will act upon an individual's request for access to his/her DRS no later than thirty (30) days after receipt of such request. If Women's Health USA is unable to act on the request within the thirty (30) day period, Women's Health USA may extend the time for response by thirty (30) days, provided that the individual is given a written notice of the reason(s) for the delay and the date by which a responsive action will be taken.

Denial of Access Notice

15. The organization will provide a timely, written denial of access to the individual when such denials occur. Denial notices will be written in easy-to-read language and will include, as a minimum, the following information:
    a. The basis for the denial of access.
    b. Any right of review (as applicable).
    c. The procedure for filing a complaint with the organization.
    d. The name and telephone number of the person to whom the complaint may be filed.
    e. The address of the U.S. Secretary of Health and Human Services.

Access to Requested Information:

16. The individual will be given access to any information requested, after excluding the information for which the organization has grounds for denying access.

Access to Requested Information Maintained Off Premises:

17. The information for which access has been requested is available off the premises or WHUSA does not maintain/retain such information, but knows where the information is located, the organization will either:
    a. Notify the individual where to direct his/her request for access, or
    b. Make arrangements for the individual to access such information. This includes, but is not limited to, information maintained by a business associate on behalf of the organization.

Violations and Enforcement: Violation of policy will be subject to disciplinary action.

Record Retention: Retention of all HIPAA covered policy information and revisions, both printed and electronic, is maintained for a period of at least six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

HIPAA Privacy Officer/Security Officer/Compliance Officer:
Refer to the *Administrative Safeguards* policy for identification of current HIPAA Privacy, Security, and Compliance Officers.

References:
§ 164.524