HIPAA Policy No. 8

Minimum Necessary and Reasonable Safeguards Policy

Policy:

8.1 Uses and Disclosures restricted to minimum necessary information

Except for uses and disclosures related to treatment of the patient (and other exceptions discussed below in paragraph 8.4), the practice must make reasonable efforts to limit the amount of patient information used within the practice or disclosed to others to that which is minimally necessary to accomplish the intended purpose of the use or disclosure.

8.2 Uses Within the Practice

For uses of information within the practice, the practice must identify all employees by category who need access to protected health information and identify the type of protected health information to which each category of employee needs access.

8.3 Uses and Disclosures to Third Parties

Requests that do not occur on a routine basis must be reviewed individually to determine the minimum amount of information that must be disclosed to achieve the stated purpose of the disclosure, based upon the following criteria:

- Determine whether the requestor was specific about the type of information that is needed (e.g., demographics, financial/billing, practitioner notes, information regarding fitting or device manufacturer).
- If the requestor was not specific, ask the requestor specifically what information is needed and why.
- If the requestor requests the entire record, ask the requestor to justify why the entire record is needed. Employees should not disclose an entire record until satisfactory justification is provided by the requestor.
- Determine whether the requestor a person who can be relied upon (as set forth in paragraph 8.5 below).
- If the requestor is a person whose representations can be relied upon, then the employee may disclose the requested information.
- If the requestor is not a person whose representations can be relied upon, and the employee has any question regarding the appropriateness of the scope of the request, the employee should ask the Privacy Officer for approval to disclose the information.

For requests that the practice receives on a routine or recurring basis, the practice should develop a specific written protocol setting forth the information which may be disclosed.

8.4 Exceptions to minimum necessary requirements

The minimum necessary restriction does not apply under the following circumstances:

- When the disclosure is made to a provider for the purpose of **treatment**
- When the patient requests his or her **own information**
- When the patient signs an **authorization** for the disclosure
- When a disclosure is made because it is **required by law**, including those disclosures required by the HIPAA regulations.

8.5 Requestors who can be relied upon to determine minimum necessary information

- When making a permissible disclosure to a public official the practice may rely on the public official's representations regarding the amount of information needed.
- When making a disclosure to another covered entity (e.g. a provider, health plan or clearinghouse) the practice may rely on the requestor's representations regarding the amount of information needed.
- The practice may rely upon the professional judgment of a business associate to determine what information is needed for the performance of professional services (for example, an accountant or attorney).

8.6 Verification of Requestor

Employees should take reasonable steps to verify the identity of a requestor if the employee does not know the requestor.

8.7 Application of the minimum necessary rule where the practice is the requestor

The minimum necessary rule also applies when the practice is making requests. The practice is required to restrict requests for information from other covered entities to the minimum necessary to achieve the intended purpose of the requested disclosure. Requests for protected health information should be made subject to the following criteria:

- Requests should be as specific as possible with respect to the amount of information needed.
- Requests should not be for entire medical records unless absolutely necessary.
- If the information is being requested for treatment purposes, the entire medical record may be requested.
- Employees should be prepared to provide justification for the scope of the request.

8.8 Reasonable Safeguards

As discussed above, all forms of communications must be limited to that which is minimally necessary to achieve the intended purpose. Reasonable safeguards must be taken to prevent disclosure of information beyond that which is minimally necessary and to prevent disclosure of information to persons who do not need the information to perform their job function.

The practice must make reasonable efforts to prevent uses and disclosures of protected health information that are not permitted by the Privacy Rule. This includes having reasonable administrative, technical and physical safeguards in place to prevent such impermissible uses and disclosures. In determining what safeguards are "reasonable", the practice will use the viewpoint of a prudent health care professional.

Some of the reasonable safeguards the practice will take include:

- Employees are responsible for taking reasonable precautions to keep medical records or other documents containing patient information out of the view of other patients or other individuals not authorized to see the documents.
- Employees are responsible for avoiding talking about patients outside of the practice when not necessary for performing their job (for example, at restaurants during lunch hour).
- Employees may not discuss patients on social media sites.
- Employees are responsible for locking away protected health information as applicable.
- Employees are responsible for securing and putting medical records and other patient information away at the end of the day.
- Employees who work in the office are responsible for supervising patients, family members and visitors within the office.
- Employees are responsible for taking precautions and using judgment when leaving messages on answering machines (e.g. if it is necessary to leave a message on an answering machine, confirm the number and leave only a minimal amount of information necessary to convey the message).
- Any mailed communications will be sent in envelopes.
- Employees are responsible for following the practice's HIPAA Security policies with regard to all electronic protected health information.
- Employees are not permitted to discuss patients on social media even if names are not discussed.
- Employees will only fax information when it is necessary for treatment, payment or health care operations and when fax number has been carefully confirmed.
- All fax communications will have a cover sheet informing the recipient that the fax may contain confidential information and contact information in the event the information is received in error.
- Any misdirected faxes will be reported to the Privacy Officer immediately and steps will be taken to mitigate any potential harm (e.g., the recipient will be called and asked to destroy the information).

Procedures:

1. Employees should be informed of their level of access by the Privacy Officer, including access to paper information and electronic information (e.g., some employees may not be permitted access to medical records). If an employee thinks that he or she needs a different level of access to perform his or her job, the employee is responsible for communicating this to the Privacy Officer.

2. When an employee receives a request for information, he or she should use the criteria set forth in paragraph 8.3 to determine whether the disclosure should be made as requested.
3. If the identity of the requestor is not known, the employee should take reasonable steps to verify the identity.
4. If an employee makes a request for information from another covered entity, the request should be specific and limited in scope consistent with the criteria set forth in paragraph 8.7.
5. Employees are responsible for following all precautions set forth above in 8.8, following the HIPAA Security Policies and will be expected to act prudently with regard to taking other reasonable safeguards to protect electronic protected health information as may be deemed necessary by the employee.
6. Employees who are uncertain regarding the scope of precautions that should be taken should seek advice from the Privacy Officer or the Security Officer.

Authorities:
45 CFR §164.530 (c)
45 CFR §164.514