

## **Disclosing and Requesting only the Minimum Amount of Protected Health Information Necessary**

### **Purpose**

[ORGANIZATION] is committed to ensuring the privacy and security of patient health information. While patient information must be available to health care professionals in the process of ensuring proper care, we should avoid disclosing more patient information than needed to perform our respective duties. To support our commitment to patient confidentiality, [ORGANIZATION] will ensure that the appropriate steps are taken to disclose only the minimum amount of protected health information necessary to accomplish the particular use or disclosure, as required under 45 C.F.R. §164.502(b), and other applicable federal, state, and/or local laws and regulations.

### **Policy**

1. [ORGANIZATION] employees will follow proper procedures to ensure that only the minimum amount of patient health information necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.
2. [ORGANIZATION] employees will request only the minimum amount of patient health information necessary to accomplish the specific purpose of the request.
3. This policy does not apply to the following uses or disclosures:
  - (a) disclosure to or requests by a provider for treatment;
  - (b) uses or disclosure made to the individual who is the subject of the information;
  - (c) uses or disclosure pursuant to an authorization initiated by the individual who is the subject of the information;
  - (d) disclosure made to the Department of Health and Human Services;
  - (e) uses or disclosures required by law; and
  - (f) uses or disclosure required for compliance with applicable laws and regulations.

### **Procedures**

1. All proposed uses or disclosures of patient health information will be reviewed by persons having an understanding of [ORGANIZATION]'s privacy policies and practices, and sufficient expertise to understand and weigh the necessary factors.
2. [ORGANIZATION] will only use, disclose, or request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.
3. Within [ORGANIZATION], the following classes of personnel require and will maintain the indicated levels of access to protected health information on a routine basis to appropriately accomplish their duties and responsibilities:
  - (a) [Medical Records] Personnel

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*

- (1) [complete access] to [clinical operation] record set; condition =
  - (2) [complete access] to [case management] record set; condition =
  - (3) [partial access] to [patient accounts] record set; condition =
  - (4) ...
- (b) [Reimbursement] Personnel
- (1) [complete access] to [clinical operation] record set
  - (2) [complete access] to [case management] record set
  - (3) [partial access] to [patient accounts] record set
  - (4) ...
- (c) [Case Management] Personnel – [partial access]
- (d) [Medical/Clinical] Personnel – [selective access]
- (e) [Dietary/Nutrition] Personnel – [partial access]
- (f) ...
4. Access to protected health information will be reasonably limited to that described in Procedure #3 by utilizing [access control systems].
  5. The following criteria will be used in limiting the amount of protected health information requested, used, or disclosed by [ORGANIZATION] personnel:
    - (a) Does the requesting individual have complete understanding of the purpose for the request, use, or disclosure of the protected health information?
    - (b) Are all of the individuals identified for whom the use or disclosure of the protected health information is required?
  6. Requests for disclosures of protected health information will be reviewed on an individual basis in accordance with criteria listed in the policy.
  7. [ORGANIZATION] Personnel [MAY] reasonably rely on requests by:
    - (a) public health and law enforcement agencies in determining the minimum necessary information for certain disclosures;
    - (b) other covered entities in determining the minimum necessary information for certain disclosures; or
    - (c) by a professional who is a member of its workforce or is a business associate of [ORGANIZATION] for the purpose of providing professional services to [ORGANIZATION], if the professional represents that the information requested is the minimum necessary for the stated purpose.

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*

8. In the event of disclosures for research purposes, [ORGANIZATION] will review the documentation of required Institutional Review Board or other approval in determining the minimum amount of protected health information necessary.
9. Knowledge of a violation or potential violation of this policy must be reported directly to the [Privacy Officer] or [Compliance Officer], or to the employee compliance hotline.

### **Regulatory Authority**

#### **45 C.F.R. §§164.502(b) & 164.514(d)**

§164.502(b) Standard: minimum necessary. (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

- (i) Disclosures to or requests by a health care provider for treatment;
- (ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under §164.508 [uses and disclosures for which an authorization is required], except for authorizations requested by the covered entity under §164.508(d), (e), or (f) [authorizations requested by covered entity for (d) its own uses and disclosures, (e) disclosure by others, (f) uses and disclosures of protected health information for research that includes treatment];
- (iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
- (iv) Uses or disclosures that are required by law, as described by §164.512(a); and
- (v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

§164.514(d)(1) Standard: minimum necessary requirements. A covered entity must reasonably ensure that the standards, requirements, and implementation specifications of §164.502(b) and this section relating to a request for or the use and disclosure of the minimum necessary protected health information are met.

(2) Implementation specifications: minimum necessary uses of protected health information. (i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*

(3) Implementation specification: minimum necessary disclosures of protected health information. (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under §164.512 [ uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required], if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of §164.512(i) [uses and disclosure for research purposes] have been provided by a person requesting the information for research purposes.

(4) Implementation specifications: minimum necessary requests for protected health information. (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must review the request on an individual basis to determine that the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

(5) Implementation specification: other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

### ***Analysis, Background, and Implications***

For all uses and many disclosures and requests for disclosures from other covered entities, the rule requires covered entities to implement policies and procedures for “minimum necessary” uses and disclosures. Disclosures to or requests by a health care provider for treatment purposes are not subject to the minimum necessary standard (see §164.502).

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*

Specifically (and as further described below), the Privacy rule establishes a requirement for covered entities to implement policies and procedures that restrict access and uses based on the specific roles of members of the covered entity's workforce. Routine disclosures are not subject to individual review; instead, covered entities must implement policies and procedures to limit the protected health information in routine disclosures to the minimum necessary to achieve the purpose of that type of disclosure. Exclusions from the standard include disclosures for individuals' access to information about themselves, pursuant to an authorization initiated by the individual, and for enforcement of this rule, as required by law.

Covered entities must make reasonable efforts to use or disclose or to request from another covered entity, only the minimum amount of protected health information required to achieve the purpose of a particular use or disclosure.

#### *Uses of Protected Health Information*

A covered entity must implement policies and procedures to identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties, the category or categories of protected health information to which such persons or classes need access, and the conditions, as appropriate, that would apply to such access. Covered entities must also implement policies and procedures to limit access to only the identified persons, and only to the identified protected health information. The policies and procedures must be based on reasonable determinations regarding the persons or classes of persons who require protected health information, and the nature of the health information they require, consistent with their job responsibilities.

For example, a hospital could implement a policy that gave nurses access to all protected health information of patients in their ward while they are on duty. A health plan could permit its underwriting analysts unrestricted access to aggregate claims information for rate setting purposes, but require documented approval from its department manager to obtain specific identifiable claims records of a member for the purpose of determining the cause of unexpected claims that could influence renewal premium rate setting.

The "minimum necessary" standard is intended to reflect and be consistent with, not override, professional judgment and standards. For example, it is expected that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed.

#### *Disclosures of Protected Health Information*

For any type of disclosure that is made on a routine, recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that permit only the disclosure of the minimum protected health information reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. Instead, these policies and procedures must identify the types of protected health information to be disclosed,

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*

the types of persons who would receive the protected health information, and the conditions that would apply for such access. Disclosures to health care providers for treatment purposes are not subject to these requirements.

The rule recognizes that specific disclosures within a type may vary, and requires that the policies address what is the norm for the type of disclosure involved. For example, a covered entity may decide to participate in research studies and therefore establish a protocol to minimize the information released for such purposes, e.g., by requiring researchers requesting disclosure of data contained in paper-based records to review the paper records on-site and to abstract only the information relevant to the research. Covered entities must develop policies and procedures (which may be standard protocols) to apply to disclosures to routinely hired types of business associates. For instance, a standard protocol could describe the subset of information that may be disclosed to medical transcription services.

For non-routine disclosures, a covered entity must develop reasonable criteria for determining, and limiting disclosure to, only the minimum amount of protected health information necessary to accomplish the purpose of the disclosure. They also must establish and implement procedures for reviewing such requests for disclosures on an individual basis in accordance with these criteria.

Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies that specifically justify why the entire medical record is needed. For instance, disclosure of all protected health information to an accreditation group would not necessarily violate the regulation, because the entire record may be the "minimum necessary" for its purpose; covered entities may establish policies allowing for and justifying such a disclosure. Disclosure of the entire medical record absent such documented justification is a presumptive violation of this rule.

#### *Requests for Protected Health Information*

For requests for protected health information from other covered entities made on a routine, recurring basis, the requesting covered entities' policies and procedures may establish standard protocols. Those protocols must describe what information is reasonably necessary for each type of request and limit the requests to only that information, in lieu of making this determination individually for each request. For all other requests, the policies and procedures must provide for review of the requests on an individualized basis. A request by a covered entity may be made in order to obtain information that will subsequently be disclosed to a third party, for example, to obtain information that will then be disclosed to a business associate for quality assessment purposes. Such requests are subject to this requirement.

Covered entities' policies and procedures must provide that requests for an entire medical record will not be made except pursuant to policies that specifically justify why the entire medical record is needed. For instance, a health plan's request for all protected health information from an applicant for insurance would not necessarily violate the regulation, because the entire record may be the "minimum necessary" for its purpose. Covered entities may establish policies allowing for

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*

and justifying such a request. A request for the entire medical record absent such documented justification is a presumptive violation of this rule.

#### *Reasonable Reliance*

A covered entity may reasonably rely on the assertion of a requesting covered entity that it is requesting the minimum protected health information necessary for the stated purpose. A covered entity may also rely on the assertions of a professional (such as attorneys and accountants) who is a member of its workforce or its business associate regarding what protected health information he or she needs in order to provide professional services to the covered entity when such person represents that the information requested is the minimum necessary. Covered entities making disclosures to public officials that are permitted under §164.512 may rely on the representation of a public official that the information requested is the minimum necessary.

#### *Uses and Disclosures for Research*

In making a minimum necessary determination regarding the use or disclosure of protected health information for research purposes, a covered entity may reasonably rely on documentation from an Institutional Review Board or privacy board. Such documentation must describe the protected health information needed for research and be consistent with the requirements of §164.512(i), “Uses and Disclosures for Research Purposes.” A covered entity may also reasonably rely on a representation made by the requestor that the information is necessary to prepare a research protocol or for research on decedents. The covered entity must ensure that the representation or documentation of IRB or privacy board approval it obtains from a researcher describes with sufficient specificity the protected health information necessary for the research. Covered entities must use or disclose such protected health information in a manner that minimizes the scope of the use or disclosure.

#### *Standards for Electronic Transactions*

Covered entities are not required to apply the minimum necessary standard to the required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard transactions in the Transactions Rule. The standard does apply for uses or disclosures in standard transactions that are made at the option of the covered entity.

*This document and the information contained therein are intended for illustrative purposes only. No information contained within this document constitutes legal advice and should not be relied upon as a substitute for legal advice or business advice or consulting services.*