

MINIMUM NECESSARY
[45 CFR " 164.502(b), 164.514(d)]

General Requirement

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do not apply to the following:

- C Disclosures to or requests by a health care provider for treatment purposes.
- C Disclosures to the individual who is the subject of the information.
- C Uses or disclosures made pursuant to an authorization requested by the individual.
- C Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.
- C Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
- C Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. We understand this guidance will not answer all questions pertaining to the minimum necessary standard, especially as applied to specific industry practices. As more questions arise with regard to application of the minimum necessary standard to particular circumstances, we will provide more detailed guidance and clarification on this issue.

Uses and Disclosures of, and Requests for PHI

For uses of PHI, the policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification.

For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit PHI disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required.

For non-routine disclosures, covered entities must develop reasonable criteria for determining, and limiting disclosure to, only the minimum amount of PHI necessary to accomplish the purpose of a non-routine disclosure. Non-routine disclosures must be reviewed on an individual basis in accordance with these criteria. When making non-routine requests for PHI, the covered entity must review each request so as to ask for only that information reasonably necessary for the purpose of the request.

Reasonable Reliance

In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- C A public official or agency for a disclosure permitted under ' 164.512 of the rule.
- C Another covered entity.
- C A professional who is a workforce member or business associate of the covered entity holding the information.
- C A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

Treatment Settings

We understand that medical information must be conveyed freely and quickly in treatment settings, and thus understand the heightened concern that covered entities have about how the minimum necessary standard applies in such settings. Therefore, we are taking the following steps to clarify the application of the minimum necessary standard in treatment settings. First, we clarify some of the issues here, including the application of minimum necessary to specific practices, so that covered entities may begin implementation of the Privacy Rule. Second, we will propose corresponding changes to the regulation text, to increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high quality health care. We understand that issues of this importance need to be addressed directly and clearly to eliminate any ambiguities.

Frequently Asked Questions

Q: How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

A: The Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the rule requires covered entities to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not a strict standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers today to limit the unnecessary sharing of medical information.

The minimum necessary standard is intended to make covered entities evaluate their practices and enhance protections as needed to prevent unnecessary or inappropriate access to PHI. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, we expect that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately will limit access to personal health information without sacrificing the quality of health care.

Q: Won't the minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

A: No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

The Privacy Rule provides the covered entity with substantial discretion as to how to implement the minimum necessary standard, and appropriately and reasonably limit access to the use of identifiable health information within the covered entity. The rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity can develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

Q: Do the minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training?

A: No. The definition of health care operations in the rule provides for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers. Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records.

Q: Must minimum necessary be applied to disclosures to third parties that are authorized by an individual?

A: No, unless the authorization was requested by a covered entity for its own purposes. The Privacy Rule exempts from the minimum necessary requirements most uses or disclosures that are authorized by an individual. This includes authorizations covered entities may receive directly from third parties, such as life, disability, or casualty insurers pursuant to the patient's application for or claim under an insurance policy. For example, if a covered health care provider receives an individual's authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of § 164.508.

However, minimum necessary does apply to authorizations requested by the covered entity for its own purposes (see § 164.508(d), (e), and (f)).

Q: Are providers required to make a minimum necessary determination to disclose to federal or state agencies, such as the Social Security Administration (SSA) or its affiliated state agencies, for individuals' applications for federal or state benefits?

A: No. These disclosures must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements. Further, use of the provider's own authorization form is not required. Providers can accept an agency's authorization form as long as it meets the requirements of § 164.508 of the rule. For example, disclosures to SSA (or its affiliated state agencies) for purposes of determining eligibility for disability benefits are currently made subject to an individual's completed SSA authorization form. After the compliance date, the current process may continue subject only to modest changes in the SSA authorization form to conform to the requirements in § 164.508.

Q: Doesn't the minimum necessary standard conflict with the Transactions standards? Does minimum necessary apply to the standard transactions?

A: No, because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the subchapter. This includes all data elements that are required or situationally required in the standard transactions. However, in many cases, covered entities have significant discretion as to the information included in these transactions. This standard does apply to those optional data elements.

Q: Does the rule strictly prohibit use, disclosure, or requests of an entire medical record? Does the rule prevent use, disclosure, or requests of entire medical records without case-by-case justification?

A: No. The Privacy Rule does not prohibit use, disclosure, or requests of an entire medical record. A covered entity may use, disclose, or request an entire medical record, without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes. In making non-routine requests, the covered entity may also establish and utilize criteria to assist in determining when to request the entire medical record.

The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment or disclosures to the individual.

Q: In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigns of office space and upgrades of computer systems, in order to comply with the minimum necessary requirements?

A: No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or

records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the rule.

Q: Do the minimum necessary requirements prohibit covered entities from maintaining patient medical charts at bedside, require that covered entities shred empty prescription vials, or require that X-ray light boards be isolated?

A: No. The minimum necessary standards do not require that covered entities take any of these specific measures. Covered entities must, in accordance with other provisions of the Privacy Rule, take reasonable precautions to prevent inadvertent or unnecessary disclosures. For example, while the Privacy Rule does not require that X-ray boards be totally isolated from all other functions, it does require covered entities to take reasonable precautions to protect X-rays from being accessible to the public. We understand that these and similar matters are of special concern to many covered entities, and we will propose modifications to the rule to increase covered entities' confidence that these practices are not prohibited.

Q: Will doctors' and physicians' offices be allowed to continue using sign-in sheets in waiting rooms?

A: We did not intend to prohibit the use of sign-in sheets, but understand that the Privacy Rule is ambiguous about this common practice. We, therefore, intend to propose modifications to the rule to clarify that this and similar practices are permissible.

Q: What happens when a covered entity believes that a request is seeking more than the minimum necessary PHI?

A: In such a situation, the Privacy Rule requires a covered entity to limit the disclosure to the minimum necessary as determined by the disclosing entity. Where the rule permits covered entities to rely on the judgment of the person requesting the information, and if such reliance is reasonable despite the covered entity's concerns, the covered entity may make the disclosure as requested.

Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with the person making the request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.