Implementing the Minimum Necessary Standard

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

The minimum necessary standard in HIPAA's privacy rule requires covered entities to make reasonable efforts to limit protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

The challenge with implementing the minimum necessary standard is defining what is "reasonably necessary" and determining how minimum necessary uses, disclosures, and requests will be managed in the non-automated and automated worlds.

Regulatory Requirements

The minimum necessary standard does not apply to disclosures to or requests by a healthcare provider for treatment, uses, or disclosures made to the individual or as authorized by the individual or to the secretary of the Department of Health and Human Services (HHS) for compliance enforcement.[1]

For the minimum necessary standard, the privacy rule requires that the covered entity identify persons or classes of persons in its work force who need access to PHI and the category or categories of PHI to which access is needed and any conditions appropriate to such access. This constitutes the requirements for ensuring minimum necessary use. For **routine and recurring disclosures**, the rule requires the covered entity to implement standard protocols that limit the disclosures to the amount reasonably necessary to achieve the purpose of the disclosures. For all **other disclosures**, the covered entity must develop criteria designed to limit the PHI disclosed to the minimum necessary. Covered entities must also limit any **request** they make for PHI to that which is reasonably necessary.

This practice brief addresses a perspective for handling minimum necessary use and for offering tools to address both routine and non-routine minimum necessary disclosures and requests.

Achieving and Monitoring Adherence

Once policies and procedures to ensure minimum necessary uses and disclosures have been established, the covered entity must make reasonable efforts to limit the use of PHI in accordance with those policies and procedures. This ongoing monitoring of compliance will require culture change, training, and regular compliance monitoring.

The culture change may be the most difficult task to accomplish. In many provider settings, clinicians are used to having total access to any patient's medical record. While the minimum necessary standard does not apply to use and disclosure for treatment, the provider has a responsibility to verify that uses and disclosures are indeed for treatment purposes.

In any instance in which the identity or authority of a requestor is not known to the covered entity, section 164.514(h) of the privacy rule requires that the covered entity obtain applicable documentation, statements, or representations in support of the purpose of the request and/or identity of the requestor. Discussing with the covered entity's own clinicians the underlying purpose of the minimum necessary standard, assuring them that they will always have appropriate access to information for patient care, and recognizing the value of accountability relative to uses and disclosures should help alleviate their concerns.

Staff whose job functions involve the use of PHI should be taught how to adhere to the minimum necessary standard. While the minimum necessary principles can certainly be taught generically to all PHI users, it is probably best to blend this training into the job-specific training that the privacy rule requires. In other words, staff members who use PHI as part of their jobs should be taught what specific information they may access as part of their assigned duties and that they should not be reviewing or using other parts of the patient's medical record or other patients' records if they do not need to.

To ensure compliance with the minium necessary requirements, internal auditors, corporate compliance officers, or others may establish ongoing monitoring (such as audit trails), periodic checking on particularly vulnerable areas (such as all requests for entire medical record), and triggered reviews when there are special complaints or incidents. This compliance process would result in feedback to members of the work force on areas needing more attention and may necessitate the redesign of work processes or procedures to enhance compliance.

Minimum Necessary Uses

Automated Environment

While not directly referring to information access controls, the minimum necessary use part of HIPAA's minimum necessary standard can be supported in an automated environment by formal information access controls. Many covered entities are planning to adopt role-based access controls (RBAC) that permit only people in certain roles to access certain types of information. For example, the billing clerk may access a patient's contract and billing information but not medical history; the treating physician, on the other hand, has full access to the patient's medical history and subsequent treatment records.

Information access controls are addressed in HIPAA's proposed security rule. Information authorization, establishment, modification, and termination policies and procedures are required. These would require that a supervisor or manager specifically authorize access for a person needing to use PHI, that the person's identity is validated when access privileges are established, that when the person's job changes access privileges are modified accordingly, and that the account is removed when the person terminates.

The proposed security rule affords the covered entity a choice as to the access control model to be used. The three models include user-based access controls (UBAC) in which users must authenticate themselves but there are no constraints on what may be accessed; RBAC in which conditions of access are placed on classes of users (as described below); and context-based access controls (CBAC), which limit users to accessing information not only in accordance with their identity and role, but to the location and time in which they are accessing the information. Although the security rule provides these options, HHS espouses RBAC as the appropriate security model to safeguard health data.[2]

Further supporting RBAC is the requirement for a procedure for emergency access (sometimes referred to as "break the glass" access). This procedure is typically found in RBAC and CBAC in order to ensure that a person with limited access who has a need to know in an emergency situation can easily access required information. There is generally a special audit function associated with this emergency access that notifies the person's supervisor, patient's attending physician, or other individual with designated authority to review such accesses for their applicability.

Access controls are linked to the person's unique user identification and password or other form of "entity authentication."

Paper-based Environment

Because most covered entities are still very much in a paper-based environment, special challenges exist in applying the minimum necessary standard to uses in this environment. There is no technology to automatically apply decision rules when accessing a paper chart, billing record, x-ray film, or the many other paper documents containing PHI. Instead, users of paper-based PHI will rely more heavily on the application and interpretation of policies and procedures, and even self-policing. As a result, the development of policies and procedures to appropriately restrict the use of PHI and the need to train staff in those policies and procedures take on special importance for covered entities maintaining PHI on paper.

Policies and Procedures Needed

Constructing policies and procedures (and RBAC) to establish minimum necessary uses must identify the persons, or classes of persons, who need access to PHI to carry out their jobs:

- Start by working with each department/unit of the covered entity to examine how members of the work force currently use PHI
- Document the list of people (or job categories) that require access to PHI and the purposes and conditions under which PHI is needed. Some covered entities are documenting this using a grid approach:

- list all categories of workers on one axis
- list categories of PHI on the other axis
- make check boxes and notes regarding special conditions in each cell where those members of the work force need access to specified categories of PHI

- Determine if it would be reasonably possible to achieve the same result with de-identified data. If so, using de-identified data is the preferred strategy. If not, determine the specific PHI needed by each type of member of the work force
- Compare findings of what information is currently made available to the various members of the work force with what they need to know. Do they have access to more health information than they really require? If so, is it reasonably possible to segregate the needed information in a way that gives them only what they need? It may not always be possible or feasible to "strip out" all extraneous health information beyond what is needed. The covered entity's goal, however, should be to restrict access to what is needed, insofar as it is reasonably possible.

Note that once you have performed this exercise, you actually have both the foundation for the minimum necessary policy and procedure as well as the role definitions required for RBAC that can be applied to computerized PHI.

Example: Consider a social worker who examines patient records on the inpatient unit as part of evaluating an elderly patient for possible placement in a long-term care facility. Using the minimum necessary principles, the covered entity would determine what the social worker needs in order to perform this function.

For this function, the social worker may need access to information about the patient's current condition, needs for long-term care, basic demographic information, and insurance resources. The covered entity determines that de-identified data would not meet the needs of this member of the work force.

The covered entity then compares these needs to the information to which the social worker currently has access on the unit--the entire medical record. The covered entity then analyzes whether it is reasonably possible to limit the social worker to only a subset of the record. It may be determined that in the paper-based environment, it is not practical to remove certain subsets of information from the record to make a special report for the social worker.

However, the covered entity would use the results of the analysis to write a policy for the social work department that defines what sections of the patient record the social worker may ordinarily use in performing this placement function. The social worker should then adhere to these policies and avoid reviewing PHI out of the scope of the function being performed.

Covered entities have the latitude to define and interpret these policies and procedures to meet their particular needs. As HHS notes in its guidance on this subject, these policies and procedures should take professional judgment into account and not sacrifice quality of care in favor of iron-clad policies and procedures.[3] Covered entities must balance a respect for the privacy rights of their patients with what is reasonably possible to do, given the organization's resources and limitations.

Minimum Necessary Disclosures and Requests

Disclosure of PHI is different from use of health information. HIPAA defines disclosure as the "release, transfer, provision of access to, or divulging in any other manner PHI outside the entity holding the information." In comparison, HIPAA distinguishes use as the "sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information."

Minimum necessary disclosures to or requests from other organizations are also distinguished by their being routine or not routine. Routine disclosures are those made on a recurring basis. For example, an ambulance company may routinely be given a copy of the patient's demographic and insurance information for the company's billing purposes. Non-routine disclosures are those that are made only occasionally, such as to a public official investigating a crime.

Developing Standard Protocols for Routine Disclosures

For disclosures made on a routine or recurring basis, a covered entity must implement policies and procedures (that may be standard protocols) that limit the protected information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. These policies and procedures should be designed to balance an individual's privacy against the legitimate need for information requested by the outside entity.

To comply with this requirement, each covered entity should review the requests it routinely receives and determine the appropriate information to be disclosed in response to the request. In developing policies and procedures or standard protocols for routine disclosures, covered entities should consider discussing this issue with their major requesters to negotiate mutually agreeable disclosures.

If a requester asks for specific information (i.e., the CT scan of the chest performed on a specified date), only the information requested should be disclosed. A standard set of reports should not be disclosed in response to a request for a specified report.

Broadly stated requests (i.e., requests asking for "any and all records") should be reviewed with the requester to determine the specific information needed. Many requesters who ask for "any and all" records reduce the amount of information requested when told the amount of the copy fees for these records.

"Examples of Routine Requests and Disclosures", below, provides a table of commonly made requests and suggested approaches for disclosures. Each covered entity should evaluate its own routine disclosures and create its own set of policies and procedures.

Criteria for Making Non-Routine Disclosures

For non-routine disclosures, a covered entity must develop criteria to limit the protected information disclosed to what is reasonably needed to accomplish the purpose of the disclosure. See "Examples of Criteria for Evaluating Non-routine Disclosures", below.

It is impossible to assign scientific methodology to evaluating disclosures. Non-routine requests must be reviewed against these criteria on an individual, case-by-case basis. The criteria need to be balanced against each other. For example, if there is knowledge that the individual could be significantly harmed by a disclosure but the provider may not get reimbursed for the care, consider alternatives such as discussing alternative payment arrangements with the patient.

Screening Requests from Other Covered Entities

Under the privacy regulations, covered entities are required to limit their requests to the minimum amount of information needed to accomplish the intended purpose. Thus, one covered entity is not required to monitor the requests received from another covered entity to ensure compliance. However, the disclosing entity should require supporting documentation for any request made by another covered entity that would involve disclosure of a complete medical record, or for any disclosure that does not appear reasonable under the circumstances.

Covered entities may also rely on a requested disclosure as the minimum necessary for the stated purpose when making disclosures to public officials. The covered entity should verify the identity of such a person.

Limiting the decision making to individuals well trained in HIM affords professional judgment and consistency. While a qualified HIM professional should be able to apply institutionally agreed upon criteria to most disclosure requests, in some cases it may be best to discuss specifics with the patient's attending physician or seek representations from the person requesting the PHI.

Disclosure of an Entire Medical Record

In compliance with the HIPAA regulations, a covered entity may not use, disclose, or request an entire medical record, except where the entire medical record is specifically justified as the amount reasonably necessary to accomplish the purpose.

Redisclosure of Health Information

One of the sample criteria is the likelihood of redisclosure. A healthcare provider's records may contain information about a patient from another healthcare provider's records. Such information may be sent with a patient who is transferred or referred to a facility for definitive treatment or continuing care.

Issues often arise regarding disclosure of information from other healthcare providers. Unless otherwise required by state law or regulation, AHIMA recommends the following:

- A provider may redisclose health information from another provider if needed for the patient's continuing care and treatment. This is consistent with HIPAA's minimum necessary standard that does not apply to uses and disclosures for treatment purposes.
- If a patient requests access to health information from another provider, it should be disclosed to the patient or patient's legal representative upon written request and following the HIPAA requirements for granting access to PHI.
- Unless otherwise required by law, generally no other redisclosures should be made. In response to a subpoena or other request, the healthcare provider should not disclose information from another provider, with the exception of outside test results (such as from a reference laboratory) that have been made part of the patient's record.

Example of Constructing Minimum Necessary Policies and Procedures and RBAC

Role	**Department**	**Minimum Necessary Access To:**						
		Applications	**Views**	**Privileges***				**Sensitive Information**
				V	**P**	**W**	**S**	
Chaplain	Pastoral care	Directory	Patient name, room, bed, religion	X	X			
Clerk-billing	Patient accounting	Billing system	Demographics insurance charges diagnosis/ procedure codes	X	X	X		Medical record
Clerk-coding	Medical records							
Clerk-filing	Medical records							
Clerk-general	Human resources							
Dietician	Nutrition services							
LAN Administrator	Information services							
*Privileges: **V**iew, **P**rint, **W**rite, **S**ign								

Examples of Routine Requests and Disclosures

Requester	**Purpose**	**Disclosures***
Ambulance company	Obtain demographic and insurance information for billing	Face sheet with patient demographics and insurance information
Attorney	Evaluate individual's medical condition in support of a lawsuit	Specific information requested
Collection agency	Obtain payment on past due accounts	File of patient names, addresses, dates of service, and amount owed
Coroner	Investigate a suspicious death	Specific information requested
Disability determination	Evaluate individual's medical condition in support of disability benefits	Specific information requested

Employer	Evaluate utilization	Plan summary information (aggregate information not individually identifiable)
Employer	Evaluate drug usage for pre-employment screening	Drug test results
Insurance company	Substantiate care provided for payment	Specific information requested in claims attachment request (often anticipated and sent in advance with claim)
Life insurance company	Evaluate individual's medical condition for issuance of a life insurance policy	Discharge summaries for specified period of time
National security	Varies	Specific information requested agencies (CIA, FBI, etc.)
Police	Investigate accidents or crimes	Specific information requested
Food and Drug	Oversee the conduct of a clinical trial	Information about the clinical trial Administration
Researcher	Treating a patient in a clinical trial	Full access to the medical record for treatment purposes
School	Evaluate child's medical condition for school activities	Letter from physician or discharge summary
State data commission	Support a statewide registry	File of specific data elements requested
Workers' compensation	Evaluate individual's medical information as requested allowed by state law	Discharge summary; other specific condition for benefits
*Documents listed are those typically found in an inpatient medical record. Documents with similar content should be disclosed from other types of records, such as outpatient or emergency department records.		

Examples of Criteria for Evaluating Non-Routine Disclosures

1. **Specificity of request:** If request is general, narrow down the disclosure to specific documents or periods of time that would fit the purpose of the request.
2. **Purpose/importance of request:** If there is a clear purpose, disclosures should relate to the purpose. If there is not a clear purpose, it may be necessary to ask for clarification and at the same time ask for what specific disclosures are sought.
3. **Impact to patient:** a. Negatively in terms of privacy: Could the disclosure potentially harm the patient, such as introduce discrimination? b. Positively in terms of patient care: Would the disclosure help the patient?
4. **Impact to covered entity:**

a. Negatively in terms of compliance: Could the disclosure result in a wrongful disclosure lawsuit? b. Positively in terms of ability to provide quality care, obtain reimbursement: Would, for example, a claim be denied because of failure to produce information?
5. **Extent to which disclosure would extend number of individuals** or entities with access to PHI
6. **Likelihood of re-disclosure**
7. **Ability to achieve the same purpose** with de-identified information
8. **Technology available to limit disclosure** of PHI
9. **Cost of limiting disclosure** of PHI
10. **Any other factors** believed relevant to the determination

Prepared by

Margret Amatayakul, MBA, RHIA, FHIMSS
Mary D. Brandt, MBA, RHIA, CHE
Jill Callahan Dennis, JD, RHIA

Acknowledgment

Thanks to Jean Ahn, HIPAA project director at Yale New Haven Health System in New Haven, CT, for her review and practical suggestions, and to Tom Walsh, CISSP.

Notes

1. The minimum necessary standard is also distinguished from the confidential communication standard, which permits patients to ask that confidential communications be handled in alternative locations or by alternative means. Confidential communications pertain to discussions and other communications with patients or other members of the work force about treatment and is designed to keep legitimate communications from being overheard or seen by those without authority to have such information.

2. When responding to questions on access controls, HHS refers visitors to its Web site to the National Institute of Standards and Technology (NIST) publication NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 17, "Logical Access Control."

3. According to HHS, "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." More information is available on the HHS Office for Civil Rights Web site at www.hhs.gov/ocr/hipaa/minnec.html.

Article citation:
Amatayakul, Margret; Brandt, Mary D.; and Dennis, Jill Callahan. "Implementing the Minimum Necessary Standard (AHIMA Practice Brief)." *Journal of AHIMA* 73, no.9 (2002): 96A-F.