What's Your Designated Record Set? (HIPAA on the Job)

Save to myBoK

by Margret Amatayakul, RHIA, FHIMSS, and Pam Waymack

The HIPAA privacy rule provides individuals the right to request access to and amendment of their protected health information maintained in a designated record set (DRS). To ensure that the DRS is completely identified but excludes information that does not pertain, covered entities should adopt a definition that clearly identifies what is included and what is excluded.

Many providers may take for granted that the DRS is what is between the covers of the patient chart. However, what constitutes the chart varies by provider, setting, and health plan, and the notion of the DRS will vary as well. The privacy rule's definition is somewhat fluid: "a group of records maintained by or for a covered entity that is: [for a provider] the medical records and billing records about individuals; [for a health plan] the enrollment, payment, claims adjudication, and case or medical management record systems; or [for any covered entity] used, in whole or in part, by or for the covered entity to make decisions about individuals."

It is important to recognize that the DRS definition does not address the means or location of storage of the information. The DRS, therefore, is not necessarily information contained solely in a single repository, but very likely information located in multiple places and from multiple sources. Some of the information may even be in an outsourced location for health plans that use a disease management company, a pharmacy benefits management company, or other structures for part of their information processing.

Start with the Legal Medical Record...

There are several approaches providers can take in defining their designated record set. A good place to start is AHIMA's definition of the legal medical record.[1] Key principles in this definition are:

- the inclusion of official business record of provider
- the exclusion of source data (e.g., films, videos) unless interpretations, summarizations, or transcriptions are not available
- the exclusion of administrative data, such as authorization for release of information, vital certificate worksheets, audit trails, copies of claims, etc.
- the exclusion of derived data for purposes of accreditation and other aggregate data

The DRS shares many features with the legal medical record. First, the **DRS should not include information used for operational purposes of the organization**, such as quality improvement data. The definition of operations provided in the privacy rule is a good source of identifying what is considered operational and therefore not what constitutes treatment (or medical records) and payment (or billing records).

Another similarity the legal medical record shares with the DRS is that **guidance imposed by more stringent state laws and other regulations must be observed**. Examples of situations in which more stringent laws must be observed would include HIPAA's requirements with respect to excluding psychotherapy notes, instances in which information was created as part of a research study to which the patient has temporarily waived right to access, or instances in which information was created in anticipation of a legal action.

Like the legal medical record, the **DRS should not include copies of records from other providers**. While information from these records may have been used in making decisions about care, patients should be directed to request access to or amendment of such information from the originating provider. In fact, the provider may deny access to such information on the grounds that the information was not created by the provider. Ideally, clinicians using such information should document such use in, for example, a progress note summarizing the information reviewed.

Finally, **the content of the DRS may be in multiple locations and media**, including paper and electronic forms.

...Then Go Beyond It

Despite the similarities between the two, the legal medical record does not meet the requirements of the DRS in a few key areas.

First, **the DRS must include both medical and billing records**, thus, some of the administrative data in a provider setting, such as a claim, would be included in the DRS. For a health plan, much of the DRS will be related to billing information. Consider using the privacy rule's definitions of treatment and payment as sources for defining what is included in medical and billing records.

Second, **many covered entities would prefer not to include source data that are not interpreted, summarized, or transcribed**. While it would not be wrong to include such data, they are not likely to be retained for a long period of time nor directly accessible in a format that is easy to copy or permit a patient to review. Indeed, some of this information may be on scraps of paper, in the comment fields of claims adjudication systems, or in voice form. Keep in mind that access and amendment do not entitle an individual to alter the information. Even in the case of an amendment, much like any correction a provider or health plan makes today, an amendment should be linked to or referenced as something added but never substituted for an existing part of the business records of the covered entity.

Third, whereas the legal medical record substantiates the business function of the provider (which is the care provided to the patient), **the DRS is created to respond to patients' requests concerning the information used in making decisions about them**. While these are not mutually exclusive purposes, they are somewhat different.

Keep the Purpose in Mind

Once the DRS has been defined in terms of what it includes and excludes, the next step is to identify where the included information can be obtained (such as from the HIM department, business office, clinic, or medical management department) and in what format it may be supplied to the patient (for example viewing from a monitor or reviewing a printout only). See "Sample Designated Record Set Definition" below.

Another key consideration is when and where the DRS will be available. Many providers are concerned about giving the patient access to the DRS during the patient care encounter because it may be incomplete or it could be difficult to maintain its integrity. Indeed, the original copy of the DRS is a legal document and patients cannot remove any of its content or write in it.

The privacy rule does not specify when or where the record should be available, therefore providers should establish specific policies. However, because the purpose of the DRS is to provide access and amendment, the most important time for a patient to have such access or to make an amendment may be during an admission or other patient care encounter and while it may be incomplete.

Customer Service is Key

Defining the DRS is not the same as preparing a medical record in response to a subpoena. Its scope should be carefully considered in advance of its use. Further, the definition should be documented so that it is known to all within the organization and can be applied consistently. The underlying purpose in defining the DRS is key to determining inclusions and exclusions, and mode of access and the definition should not be created in isolation.

Understanding its purposes and the access this purpose demands must be considered. For example, providing access to an incomplete record during an admission might be discouraged, so instead, the provider could offer to review a page or portion of the record with the patient using this as an educational opportunity or even offer a summary of the record in lieu of a copy of the entire record. Likewise, it is during the claim adjudication process that an individual may be most interested in access to information retained by the health plan.

It is important to maintain a customer service attitude: the right of the patient to access information on which care or payment decisions are being based is the underlying purpose of defining the DRS. If the patient has reason to believe the DRS contains

erroneous information, it is better to permit access and amendment than for the information to go uncorrected with a harmful affect on the patient. While some requests for access and amendment may seem inappropriate, attempting to hide information can have a negative effect on the provider-patient or health plan-customer relationship.

Sample Designated Record Set Definition

Excluded items	Included items	Form supplied to patient	Source
Source data, including photographs, films, monitoring strips, videotapes, slides, and worksheets	Legal medical record, including photographs, strips, and other source data incorporated into progress notes	Copy of paper chart, printout, or summarization, view computer screen or original record with attendant only	Physician, head nurse, HIM department
Administrative data, such as audit trails, appointment schedules, and practice guidelines that do not imbed patient data	Patient-specific claim, remittance, eligibility response, and claim status response, charge screen, statement of account balance, and payment agreement	Copy of paper document or printout only	Business office
	Consent and authorization forms, Medicare ABN letter, Medicare Life Time Reserve Letter, Medicare Notice of Non-Coverage Letter, and copy of insurance card	Copy of paper document only	Business office, HIM department
Other provider records	Patient-submitted documentation and referral letters	Copy of paper chart or printout, computer screen or original record with attendant only	HIM department, physician office
Derived data	Minimum data set specific to patient	View with attendant only	HIM department
Note: When photographs are mounted within the paper medical record or embedded as an image within an electronic file, they are part of the designated record set. When photographs are maintained separately, they are not part of the designated record set.			

Note

1. Amatayakul, Margret A. “Practice Brief: Definition of the Health Record for Legal Purposes.” *Journal of AHIMA* 72, no. 9 (2001): 88A-H.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.* ***Pam Waymack*** *(pamwaymack@aol.com) is managing director of Phoenix Services Managed Care Consulting, Ltd., in Evanston, IL.*

Article citation:
Amatayakul, Margret, and Pam Waymack. "What's Your Designated Record Set?" (HIPAA on the Job series) *Journal of AHIMA* 73, no.6 (2002): 16A-C.

Driving the Power of Knowledge