Codify
BY AAPC

Health Information Compliance Alert

HIPAA Guidance: HHS OFFERS PRIVACY DOS AND DONTS

Can you charge patients for copies of their medical records? Should you get the plumber to sign a business associate contract? Is HIPAA going to eliminate that handy plastic box outside the exam room where you stash medical charts during a patients visit?

The answers to these and many other Privacy Rule questions are now available, thanks to a new Frequently Asked Questions Web page posted Oct. 8 by the **Department of Health and Human Services Office for Civil Rights**.

With the HIPAA privacy rule finalized and just six months away from enforcement, OCR answered the throng of public inquiries requesting further clarification by releasing a series of nearly two dozen questions and responses on a range of practical issues facing covered entities. Among several of the topics discussed, the FAQ page addresses the following:

How much for copies? Since the HIPAA privacy rule permits patients to request copies of their medical records, covered entities have wondered if and how much they might charge patients for these copies. According to OCRs response, the privacy rule allows covered entities to impose "reasonable, cost-based fees," that "may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed." The FAQ page goes on to note that covered entities may also impose a fee for preparing a summary or explanation of a patients protectedhealthinformationifthepatienthasagreed to receive such a format. The fee, however, may not contain any costs associated with the search or retrieval of the patients PHI.

Is genetic information protected? Simply put, genetic information is considered protected health information under the privacy rule. So long as its individually identifiable and maintained by a covered provider, health plan, or health care clearinghouse, its PHI.

"Mr. Johnson, the doctor will see you now." Wait can I even say that?!? Yes, you can, according to OCR. Covered entities such as physician offices need not abandon the longstanding practices of calling out patient names in waiting rooms or using sign-in sheets, so long as the information disclosed is "appropriately limited." The privacy rule allows for "incidental disclosures" that may occur as a consequence of an otherwise permissible disclosure i.e. a patients name being overheard by other waiting room occupants. These "incidental disclosures" are allowed to the extent and heres the key that the covered entity has "applied reasonable and appropriate safeguards," and "implemented the minimum necessary, where appropriate." Neither sign-in sheets nor waiting room call-outs should contain any information pertaining to the patients medical problem or history, thereby eliminating any inappropriate PHI-laden announcements such as, "Mr. Johnson, the doctor will now treat you for your stomach ache."

Plastic boxes breathe sigh of relief. OCR makes it clear that HIPAAs privacy rule is not aiming to eliminate another long-standing clinical practice such as placing patient charts in a plastic box outside of an exam room for the physicians convenience. The privacy rule will allow clinics to continue the "plastic box practice," so long as these covered entities implement minimum necessary standards and reasonable safety measures to protect the patients privacy. With regards to minimum necessary standards, OCR states that since "the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary standard would be satisfied." To help ensure the confidentiality of the patient chart, the FAQ page suggests employing such safeguards as "limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by."

Despair, nervousness over repair services? Unsure whether you must require technicians such as plumbers, electricians or photocopy repairers to sign business associate contracts? According to OCR, repair technicians who may perform

services within a physicians office but whose jobs do not require access to protected health information are not business associates as defined by HIPAA. The FAQ page identifies business associates as "contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information."

Do you want that cleaned or shredded? Because it does make a difference... Generally speaking, janitorial services that are hired to clean the facilities of a covered entity need not sign a business associate contract since the work typically performed does not entail the use or disclosure of protected health information. OCR asserts that "any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties and could not be reasonably prevented."

The FAQ page goes on to state, however, that if a service is hired to do work for a covered entity that would involve access to protected health information (such as the shredding of documents containing PHI), then it would likely be deemed a business associate. OCR notes that an exception in this case would be if the work (i.e. shredding) were to be performed under the direct control of the covered entity (i.e. on the covered entitys premises). In this instance, the privacy rule "permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service."

The message or the messenger? Are mail carriers your business associates? According to the FAQ response, the HIPAA privacy rule does not require covered entities to sign business associate contracts with either the United States Postal Service, or private couriers such as United Parcel Service, since such organizations simply act as "conduits" for protected health information. Because these couriers transport PHI but generally have no need or intention to access it (except as required by law), OCR maintains that "the probability of exposure of any particular protected health information to a conduit is very small," and therefore "a conduit is not a business associate of the entity."

Editors note: To view the complete HIPAA Privacy Rule FAQ page, go to www.hhs.gov/ocr/faqs1001.doc