Minding Your Information Through Document Retention Policies

By Justin Joy, JD, CIPP

The information contained in your practice's documents and records is one of the most valuable assets to your organization. Without this information, your practice cannot treat patients, receive compensation, or otherwise operate. With the fundamental transformation of documents from paper to digital form, storage costs and physical burdens of document management have reduced drastically. More impressive, however, has been the exponential growth in the amount of digital information that medical practices now create and maintain. Besides improving operational efficiencies through managing these tremendous volumes of information, implementing a document retention and destruction policy can also reduce risks to your practice.

As an initial matter, one person needs to be designated within your practice to be responsible for developing and maintaining the document retention policy. Of course, the designated individual can delegate tasks to others and can also bring in outside resources, such as an attorney, to assist. As with most other project-based efforts, designating a single individual responsible for developing, implementing, and administrating a document retention and destruction policy increases the chances that such an effort will actually come to fruition.

To properly manage your information, you must first know where the information is stored. Even in a smaller practice, taking inventory of your information can be a challenge. Gone are the days where a practice's documents are stored in a single records room. Today, data is stored on mobile devices, workstations, network servers, and removable media such as thumb drives and external hard drives. Information is also maintained by third parties such as cloud storage vendors and paper archiving services. While taking an inventory of your information can be complicated, it is important to know where your information is stored. Get your IT personnel involved in this process. There are tools available to help identify where data is stored. Also, reviewing vendor invoices and contracts may be helpful in determining which vendors store your information. (You will need HIPAA-compliant business associate agreements with each one of your vendors receiving and storing protected health information.)

Once you have identified where your data is stored, you must determine the different categories of information you have. This can also be a laborious process, but start simple. For instance, nearly every practice has certain categories of information such as patient data, employee and human resource information, tax information, corporate information,

and data pertaining to third-party contracts. Your practice may have additional categories. This exercise necessarily involves seeking input from different functions within your organization.

The next step is to determine how long the different types of documents you have need to be retained. Thoughtfulness—and perhaps seeking legal advice—in making retention period determinations is important. While the risk of destroying a document before it is no longer needed is obvious, what may not be as obvious is that retaining a document significantly longer than necessary may also create a risk. Data breaches are one risk of retaining stale documents. When your practice experiences a data breach, you must notify the patients affected by the breach. How would you like to notify a patient, whom your practice has not seen in 15 years and has moved to another city, about a data breach where a cybercriminal has stolen his or her Social Security number from a very old billing record?

Another risk of retaining information longer than necessary is the potential for an increased burden in employment litigation, contract disputes, and health care liability actions. While it is imperative you retain, subject to a "litigation hold," all documents pertinent to ongoing litigation or litigation that is reasonably anticipated, unnecessarily retaining unrelated documents may lead to increasing the inherently high costs and burdens associated with any legal action because of pre-trial discovery obligations.

Once a document has reached the end of its retention period, it must be properly destroyed. If a document is not properly destroyed, the benefit of an otherwise well-managed document retention policy is greatly diminished. Proper data destruction in today's digital world can be challenging. In a paper environment, once a paper document reaches the end of its retention period, it is simply shredded. Today, however, destroying, and not just deleting, all copies of an electronic document or record requires knowledge of every location where a copy is stored, which gets back to the initial step of taking a data inventory discussed above. Often, numerous copies of electronic documents are stored in multiple locations such as workstations, mobile devices, replicated servers, and cloud-based backup systems utilizing co-located data centers. IT personnel should be involved in developing a destruction plan to address these considerations.

A document retention and destruction policy requires thought and effort to put into place and administer, and once such a policy is put into place, it should be reviewed and updated periodically. The long-term benefits of the policy include increased efficiency and lowered risk, which are worth the short-term effort.
