Legal Perspective on the Importance of Effective Information Governance

Save to myBoK

By Ron Hedges

Editor's note: The views expressed in this column are those of the author alone and should not be interpreted otherwise or as advice.

AHIMA's newly developed Information Governance Principles for Healthcare (IGPHC)™ offer healthcare professionals an information governance (IG) framework specific to the healthcare industry. Consisting of eight principles, this framework helps establish a strong foundation of IG best practices for healthcare organizations. The eight principles are:

1. Accountability
2. Transparency
3. Integrity
4. Protection
5. Compliance
6. Availability
7. Retention
8. Disposition

The article will discuss the impact that an effective IG program—or lack thereof—can have for a healthcare organization in relation to legal considerations. For more information on IG and the IGPHC, visit AHIMA's information governance web page. AHIMA thanks ARMA International for use of the following in adapting and creating materials for healthcare industry use in IG adoption: Generally Accepted Recordkeeping Principles and the Information Governance Maturity Model. www.arma.org/principles. ARMA International 2013.

A Legal Perspective on Effective IG

Some actions that could overlap between IG and legal considerations in a healthcare organization include establishing policy, prioritizing investment, securing information assets, and determining accountability. What does this mean in the context of litigation?

In the context of litigation, IG must encompass the means to deal with litigation that is either in process or reasonably anticipated when the duty to preserve relevant information arises. IG is important in this context, as a healthcare provider cannot preserve anything appropriately unless the provider knows what information they have, where the information is, and how to preserve the information correctly. All of these things are necessary for effective IG as it relates to legal considerations for a provider.

Now, let's put effective IG into the reality of the ever-increasing volume and variety of information and data in the healthcare industry. In addition to the needs described above, having an effective IG program in place means that the provider should know specifically what protected health information (PHI) it has, where the PHI is located, and what the *current value* of the PHI is. The following offer some example scenarios to be considered in this context.

Examples of Effective IG Needs in the Context of Legal Considerations

- Assume that 80 percent of information kept by a provider falls within the provider's definition of a "record." What does the "non-record" information consist of? Why is it being retained?
- Assume that certain business-related information is defined to be a record and retained. What is the "shelf life" of that information? Why is the information retained after it has lost value?
- Assume that certain information has lost its value, but that someone within the organization retains the information in the expectation that the information may have some value in the future. What might eb the consequences of doing so?

Retaining Low-Value Information Can Become a Liability

There are a few ways that information that is retained, but has little or no value, can become a liability. Having an effective IG program in place that can identify information and its current value can help healthcare organizations mitigate the issues described below:

1. Cost
    a. Storage costs may be decreasing, but do overall storage costs increase as more information is created and retained?
    b. What if the hardware or software on which information is retained becomes unserviceable or otherwise obsolete?
2. Litigation
    a. What if the information becomes subject to a legal hold?
    b. How does a provider decide whether a "source" has information subject to a legal hold if the source cannot be accessed or can only be accessed with difficulty?
    c. The above issues might show up on the "judicial radar" if there is a possible failure to preserve the information and/or potential spoliation.
3. Embarrassment
    a. What if the information becomes public and the disclosure leads to negative consequences for the provider?
4. Data breach
    a. What if the information becomes the subject of a data breach?
    b. What should a provider do in the event of a breach?

Retention of information when there is no current known reason to retain that information can lead to "corporate amnesia," where the organization loses track of what some of its retained information represents—or why they even have it. Over-preservation of information if a duty to preserve arises can be another issue.

Ron Hedges, JD, is a former US Magistrate Judge in the District of New Jersey and is currently a writer, lecturer, and consultant on topics related to electronic information.

Original source:
Hedges, Ron. "Legal Perspective on the Importance of Effective Information Governance" (Journal of AHIMA website), August 21, 2015.

Driving the Power of Knowledge