Avoiding Sanctions through Effective Information Governance

By Ron Hedges

My prior posts have looked at AHIMA's Information Governance Principles for Healthcare™ (IGPHC) in the litigation context. In this post I want to focus on one facet of litigation, something every healthcare provider (and every other party) wants to avoid: sanctions. Specifically, the imposition of sanctions for the loss of electronically stored information (ESI). Adoption of the IGPHC can be a powerful deterrent to sanctions should ESI be lost.

First, remember that sanctions can only be imposed for the loss of ESI that is subject to a duty to preserve. Absent that duty, a court will not sanction a healthcare provider for the loss of ESI. Now recall that the Federal Rules of Civil Procedure were amended effective December 1st. One rule in particular, 37(e), underwent a substantial change. It states that if ESI is lost that "should have been preserved in the anticipation or conduct of litigation because a party failed to take reasonable steps to preserve it," certain measures can be taken if the lost ESI "cannot be restored or replaced through additional discovery." The severity of the measures can vary given the intent behind the loss of the ESI. For example, so-called "case-dispositive" measures can be only imposed if ESI is lost "with the intent to deprive another party of the information's use." But what I want to do is focus on "reasonable steps" and how the IGPHC can inform an argument that these had been taken.

We start with a maxim, *modus supra materiem,* which means that procedures are more importance than substance. What does this have to do with "reasonable steps" and the IGPHC? Quite simply, the IGPHC can assist a party which has lost ESI to demonstrate that the party had taken reasonable steps to avoid the loss and, through demonstration, avoid sanctions under Rule 37(e). Let's take the principles in the IGPHC one at a time:

Accountability:

This requires that someone be in charge of information governance. The person oversees and delegates responsibility. Being able to point to such a person should show that there are procedures in place to deal with preservation of ESI rather than having *ad hoc* responses to a duty to preserve.

Transparency:

Transparency translates into open and verifiable documentation of information governance processes and actions. This allows a showing that there are no "secret" or confusing steps in a party's preservation efforts and that what "preservation" means is understood.

Integrity:

Integrity is intended to lead to a reasonable assurance of authenticity and reliability. These characteristics can be used to demonstrate that, in the normal course, ESI is preserved in a manner that allows it to be trustworthy.

Protection:

This requires appropriate levels of security to guard against loss or corruption of ESI (and, for litigation purposes, corruption can be the same as loss). A party that can demonstrate that it has security measures in place is well-positioned to show that bypassing these measures would be extremely unlikely.

Compliance:

This has to do with meeting legal obligations. Compliance allows a party to show that it understands what is imposed by law (for our purposes, the duty to preserve) and that it has in place, among other things, mechanisms that demonstrate this understanding as well as allow appropriate monitoring.

Availability:

Availability means timely, accurate, and efficient retrieval. These characteristics can be used to show that when ESI is requested for litigation needs a party can respond to the request consistent with the processes that it has implemented in an appropriate manner.

Retention:

Retention addresses maintenance of ESI for an appropriate time. Retention carries with it the ability to retrieve and access information consistent with retention schedules. This can enable a party to demonstrate that it classifies ESI in an appropriate manner and that it understands where and how ESI is maintained.

Disposition:

Last, but not, comes disposition of ESI at the end of its lifecycle. For litigation purposes, consistency in disposition allows a party to show that it understands its retention obligations and, at the same time, appreciates the need for an "off switch" when a duty to preserve arises.

What does all this have to do with our maxim and the IGPHC? Assuming that a party has lost ESI, they will have to demonstrate that they took reasonable steps to avoid the loss. In other words, that party will have to show that it had procedures that made the loss an anomaly. Perfection is not required. The principles of the IGPHC establish a framework that a healthcare provider can use to demonstrate that sanctions should not be imposed under amended Rule 37(e) both to an adversary before it seeks an award of sanctions or to a court should the party proceed on an application to impose sanctions.

Note Regarding Additional Sanctions

This post addresses sanctions under the Federal Rules of Civil Procedure. The reader should be aware that there are other mechanisms under which sanctions for a loss of ESI might be imposed under federal law and that states have their own rules governing sanctions awards in their courts.

Acknowledgment

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. ARMA International 2013.

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

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. "Avoiding Sanctions through Effective Information Governance" (Journal of AHIMA website), February 16, 2016.
