

Certificate of Destruction: What It Is, What It's Not

Save to myBoK

by Robert Johnson

Major healthcare facilities generally choose to meet their document destruction needs through outsourcing. The certificate of destruction (COD) is virtually the universal documentation or audit trail in the outsourced security shredding world. It shows who destroyed what and when they did it.

The document varies widely in appearance. Some service providers issue a document that looks like a diploma with gold foil embossing and script fonts. Others place a simple disclaimer at the bottom of an invoice that states everything covered by the invoice has been destroyed. This article will clarify the role and purpose of the COD, as well as correct misunderstandings about its basic elements.

A False Sense of Security

The most common and dangerous misconception about the COD is that it relieves the original record owner from any further responsibility. The attitude is best expressed by the familiar sentiment, “I don’t care what they do with the records as long as I have a letter saying they were destroyed.”

However, any auditor, lawyer, judge, or jury will want to know what was done to ensure that the contractor had the capability and character to fulfill such an important task. A defense of “we got a letter saying it was destroyed” is not adequate because no client can completely transfer liability. This is why it is important to carefully select a service provider.

What’s in the Box?

Another common misconception about the COD is that it is proof of what was given to the service provider to destroy. The COD should have some degree of itemization of what is destroyed on each particular records pick-up. Records might be itemized by year, with a heading such as “All Patient Records 1995–1999.” Alternatively, it is perfectly acceptable (and reasonable) to reference a more detailed manifest as an addendum to the COD, which is attached and signed by the service provider’s agent upon removal. Remember, this itemization is not about proving what the service provider is accepting, but merely a record of what was intended to be sent to them.

The fact is that any court will rule that it is unreasonable to expect that the service provider’s agent could have any definitive knowledge of what the client is actually giving him or her. It is also unreasonable to think the client can prove that every copy of that record ever created has been similarly destroyed in a controlled environment. Short of those two necessary provisions, how could anyone prove that a particular document was in a particular box?

The practical inability to prove what is actually in any particular batch of documents is among the most compelling reasons for carefully selecting a secure and reliable information destruction contractor.

The COD’s Real Value

Consistency and documentation are the key components to a records management program’s ability to withstand legal scrutiny. If both of these components are evident in the destruction program, there is little chance that it will be construed as negligent or suspicious.

The best way to establish that consistency is to record destruction events over an extended period of time. A consistent and chronological series of CODs from a quality service provider over an extended period of time is worth its weight in gold in establishing adherence to a program and responsible destruction procedures. This practice creates great ammunition for clients

to defend against claims of suspicious destruction activity. A legacy of routinely issued CODs is also an important ingredient for establishing compliance with HIPAA and other regulatory requirements.

Elements of a COD

A COD can take many forms. It can be a single, itemized document, or it can be a series of documents generated from individual records pick-ups. When pulled together, individual records constitute all the necessary elements of a COD. The good news is that almost any of those forms can be easily modified to give the client the required information.

In order for a COD to do what it does best, it should establish the following:

- **Unique and serialized transaction number**—each records pick-up or batch should have a unique transaction number that follows it through any system.
- **Acknowledgment of transfer of custody**—the work order should include a space where the client's authorized representative acknowledges that he or she is handing over the materials for the purpose of destruction. It should also reference the date of the transfer and the location.
- **Reference to the terms and conditions**—the COD should include a provision that refers to the policies and procedures mutually agreed to by the client and service provider, which govern the handling and processing of records during the destruction process. The service provider's COD is not constructed specifically for the healthcare client. The reference to the terms and conditions is what links the COD to the business associate agreement, since those same terms and conditions should be reflected there as well.
- **Acceptance of fiduciary responsibility**—the service provider's agent should be required to sign a statement confirming that all records accepted are considered confidential and are to be transported or processed as such, as specified in the terms and conditions, contract, or service agreement.
- **Date the information ceased to exist**—for mobile services, this is fairly simple and can be provided on the spot. For plant-based services, it must be completed at the facility as the paperwork follows the material through the process.
- **Location of the destruction**—in the case of plant-based services, this is the address of the service provider's destruction facility. In the case of mobile shredding service, it is the client's address.
- **Witness to destruction**—the COD should require a witness to sign a statement attesting that the records, as represented in the work order, were destroyed on the date and at the location as indicated in the COD. Legally, the witness does not have to be an employee of the client, based upon the combination of the previously mentioned "transfer of custody" and "acceptance of fiduciary responsibility" provisions. A duly authorized representative from the document destruction service is perfectly acceptable given the transfer of custody and the acceptance of the fiduciary responsibility described earlier.

Worst Case Scenario—And How to Handle It

In a worst-case scenario, where protected health information entrusted to a document destruction service surfaces at a later date causing both embarrassment and legal proceedings, the COD will be very important in establishing responsibility for the mishandling and liability for the consequences. If it can be clearly established that the contractor was the cause of the unauthorized release and the provisions of a COD recommended in this article are present, there should be no trouble determining that the contractor is responsible.

However, the courts are also likely to consider the due diligence of the process used to select the vendor. Requiring the provisions described here will make a case for the application of due diligence. So will the answer to the question, "What was your procedure for selecting a contractor for this critical function?"

What happens after culpability is established largely depends upon the insurance coverage of the service provider. (AHIMA's practice brief "The Destruction of Patient Health Information" recommends liability provisions be included in any service contract to outsource document destruction.¹)

Don't Shoot the Messenger, Spread the Message

The COD is a very important and necessary document, but it is not a “get out of jail free” card. No organization can pass on its responsibility to protect the information with which it was originally entrusted. In the case of document destruction services, that responsibility can only be reflected in the care taken when selecting the service provider and crafting their requirements.

Note

1. AHIMA. “Destruction of Patient Health Information.” November 2002. Available online in AHIMA’s FORE Library: HIM Body of Knowledge at www.ahima.org.

Robert Johnson (exedir@naidonline.org) is the executive director of the National Association for Information Destruction in Phoenix, AZ.

Article citation:

Johnson, Robert. "The Certificate of Destruction: What It Is, What It's Not." *Journal of AHIMA* 76, no.6 (June 2005): 54-55,59.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.