

## Information Destruction Programs: How You Can Defend Them and They Can Defend You

by Robert J. Johnson

Death and taxes are often jokingly referred to as the only sure things in life. However, for the purposes of this article, I'd like to offer three additional scenarios:

1. Hard-copy records of patient information will be created in abundance and in many different forms.
2. Those records will eventually outlive their usefulness—some in days, others in years—and will require destruction.
3. Procedures to protect discarded patient information will eventually be put to the test.

To say that HIPAA has healthcare professionals and institutions evaluating how they handle patient data at every stage is an understatement. Therefore, it is appropriate to consider elements of an information destruction program necessary in order for it to deliver the desired protection.

### For the Records

An information destruction program should include secondary, incidental, and stored records. The best place to begin building a thoughtful, comprehensive information destruction program is to determine what documents it should cover. It is very common to concentrate a program on documents that are neatly tucked away on shelves in file rooms and warehouses. However, secondary and incidental records also constitute a significant risk to patient privacy.

Documents such as duplicate pages of forms, misprints, copies of billing statements, hand-written memos, dietary menus, prescription slips, and appointment schedules are examples of incidental records that contain patient information that should be protected by the same physical safeguards afforded to stored records when they are discarded.

### Under Lock and Key

Secure collection containers should be used for the collection of discarded

information. It is easy enough to lock warehouses, storerooms, and file cabinets to protect stored records. However, when a record is discarded — especially an incidental or secondary medical record — it is often deposited in unlocked or open bins, sometimes even outside with public access.

Of course, once those incidental records are recognized as documents containing patient information, the danger of this practice is apparent. If it is information requiring destruction, it must be protected at every point, and the use of unlocked or open receptacles to collect it is not prudent.

### Getting the Job Done

There should be specified, documented criteria used as the basis of selecting an information destruction

**Everyone from risk managers and insurance companies to government regulators and investigative reporters will be testing the system. If a program has holes in it, that is when they will become apparent.**

contractor. It is safe to say that the use of information destruction contractors is the prevailing method for institutions to destroy discarded media. However, the reality is there are no regulations governing this service and security procedures can vary considerably. And while some contractors do fraudulently represent their security standards, it is more likely a problem would result from undisciplined practices. Therefore, it is important to specify what is required of the contractor in the selection process.

Among the items to be required of an information destruction contractor are employee screening, appropriate insurance,

written procedures, access prevention, monitoring and alarm systems, specific particle size, and a custodial audit trail. Since the vendor for this service has the status of business associate as defined by HIPAA, these points should be included as addendums to the requisite contract.

The main reason for establishing criteria for selecting an information destruction contractor is that the due diligence of the selection process must be apparent and defensible in the event that those physical safeguards are ever breached, audited, or challenged.

Among the “sure things” introduced at the beginning of this article was the statement that procedures to protect discarded patient information will eventually be put to the test. At this point in time, HIPAA compliance is a goal. In less than a year, it will be a requirement. Everyone from risk managers and insurance companies to government regulators and investigative reporters will be testing the system. If a program has holes in it, that is when they will become apparent.

HIPAA is about privacy protection but is also about accountability. Those accountable for the protection of patient information had better, at the very least, be able to defend their decisions when the system is put to the test.

**Robert J. Johnson** is the Executive Director of the National Association for Information Destruction, Inc. For more information, contact NAID by e-mail at [exedir@naidonline.org](mailto:exedir@naidonline.org), or visit NAID's Web page at [www.naidonline.org](http://www.naidonline.org).

Copyright © 2002 by the American Health Information Management Association. All rights reserved. No part of this publication may be reproduced, reprinted, stored in a retrieval system, or transmitted, in any form or by any means, electronic, photocopying, recording, or otherwise, without the prior written permission of the association.

Reprinted by the National Association for Information Destruction, Inc., with permission of AHIMA for use by NAID Members Only.