A Publication of the American Health Lawyers Association
Health Information & Technology Practice Group

Volume 11
Issue 1
February 2008

HIT News

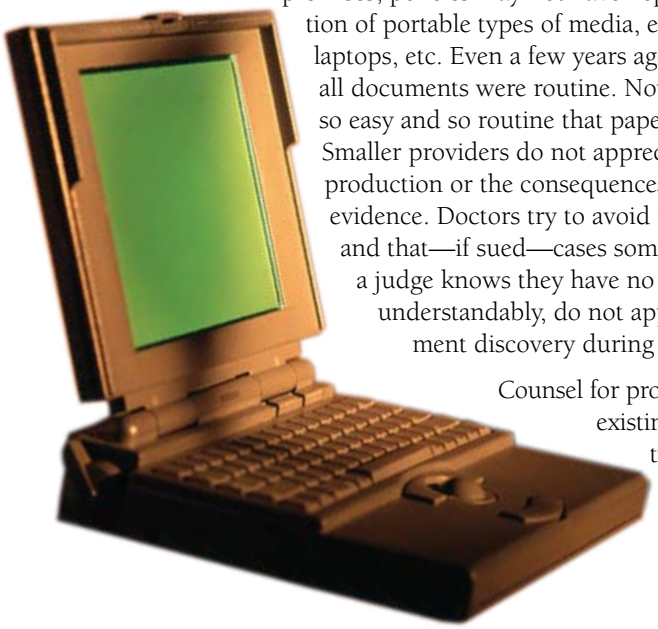
Preparing for Litigation—Before It Strikes*

James Rosenblum, Esquire
Rosenblum Newfield LLC
Stamford, Connecticut

I. Introduction

When you mention "records" to healthcare providers—and especially their office administrators—they think "electronic medical records . . . HIPAA . . . computer systems . . . security vendors . . . incomprehensible terms and acronyms . . . huge expenses . . . disclosures nobody reads and nobody understands" and, alas, "aspirin." Their lawyers, however, have nightmares about retrieving electronically hidden material on computer discs, flash drives, PDAs, or back-ups, not to mention finding venders to re-create "e-records." They also are concerned about spoliation of evidence, making "frivolous" claims indefensible. The purpose of this article is to provide strategies to help lawyers persuade medical practices to address these problems and to provide practical, workable advice for dealing with them, which also may translate to other providers, including hospitals.

Medical practices (and other healthcare providers) tend to be resistant to preventive legal advice for a host of reasons. They view it as a huge expense without value. They believe they dealt with "the record problem" by enhancing privacy, confidentiality and security, and establishing Health Insurance Portability and Accountability Act (HIPAA)-mandated procedures and forms. They assume business associate contracts and notice of privacy practices are sufficient for all record-keeping purposes. Even where providers have good procedures for computers on premises, policies may not have kept pace with the proliferation of portable types of media, e.g., PDAs, flash drives, laptops, etc. Even a few years ago, paper copies of virtually all documents were routine. Now, scanning documents is so easy and so routine that paper records are declining. Smaller providers do not appreciate the difficulty of record-production or the consequences if accused of spoliation of evidence. Doctors try to avoid thinking they will get sued and that—if sued—cases somehow will go away, once a judge knows they have no merit. Medical practices, understandably, do not appreciate the scope of document discovery during litigation.



Counsel for providers need to explain that existing safeguards have limitations, that compliance with HIPAA does not mean that the records problem has been solved, and that business records agreements

Table of Contents

AMERICAN HEALTH LAWYERS ASSOCIATION

address important issues but not necessarily the types of issues that are likely to arise in litigation. They need to emphasize the unpredictability of litigation, the cost of record production without anticipatory planning, and the "cost" of inability to produce records. Medical practices need to plan for litigation. Such planning may be accomplished in a simple, cost-effective way.

Anticipatory planning involves preparing an inventory and a few key policies, which address the following:

- What records are maintained
- How records should be defined, and why they should be defined
- Possession, control and storage
- Format
- Policies and mechanism for back-ups
- Modification of records
- Policies for maintaining and destroying, records

II. What Records Are Involved?

Apart from the fact that records may be maintained in different places and in different formats, the term "records" itself is ill-defined. Even traditional "patient records," "medical records," or "the chart" include different things, e.g., pathology slides, radiology studies, lab tests, and billing records. When records exist on computers, they often are referred to as "data" or "files."

The inventory should specify the types of records, insofar as possible, including:

- Clinical records, e.g., histories, physical examinations, progress notes, consultation reports, and hospital records
- Patient communications
  - Voicemails
  - Telephone call message pads
  - Emails
- Pharmacy records, including orders and prescriptions
- Laboratory records
- Radiology reports and images
- Pathology reports and slides
- Billing and health insurance records
- Employment records
  - Employment applications
  - Payroll records
  - Office manuals, policies and procedures
  - Pension plans
- Contracts, including those with health insurers and vendors
- Business associate contracts
- Partnership/shareholder agreements
- Financial records, e.g., accounting, tax records, and bank records
- Insurance, other than health insurance, including liability insurance, business operations insurance, etc.

III. Defining "Records"

Since the term "records" is vague, it makes sense to define specified record sets. For example, "clinical records" could include histories, physical exams and progress notes, but not consultations, hospital records, or billing records. Similarly, an employee's "personnel file" may include evaluations but not more sensitive medical information.

IV. Storage, Possession, and Control

The inventory should include locations where records are maintained. For example:

- Centralized computers, e.g., "servers" controlled or maintained by providers
- Individual computers or media devices controlled or maintained by employees, e.g., desk top computers, home computers, laptops, CD-ROMs, DVDs, and flash drives
- Personal digital assistants, e.g., Treos, Blackberries
- Third parties, e.g., hospitals, insurers, laboratories, pharmacies, and vendors (e.g., medical supply companies), payroll companies
- Insurers, including liability, health, and business insurers
- Management companies
- Consultants, e.g., accountants, lawyers, and benefit administrators

For current patients, it usually is relatively easy to retrieve relevant information. When patient care ends or employees leave, however, it may not be clear who has possession and control of records, or whether those records can be accessed in the future, or the costs of obtaining records. Therefore, the inventory should specify who has responsibility for maintaining and locating such records. Ideally, the inventory also should address other types of concerns addressed in this article, including the format of information, back-ups, modification of records, and destruction of records.

V. Format

Listing the format of data is important because of all the possible formats and because formats change and become obsolete. Potential formats include:

- Office-based software, which often needs to be updated
- Web-based applications
- CD-ROMs
- DVDs
- Tapes
- Voice recordings
- Videos
- Paper records

As formats evolve, or become outdated, consideration should be given to determining whether and how to update records.

VI. Back-Ups

Records always are subject to inadvertent destruction. Paper records stored in basements succumb to floods. Probably everyone has lost computer files. Most businesses have back-up systems, but these do not control records maintained by other people or entities in different formats. The issues to address include:

- Who makes back-ups?
- What is the format of the back-ups?
- Where are back-ups stored?
- How are back-ups retrieved?
- Can the date of back-ups be controlled, i.e., can back-ups reproduce data as of a specific date? If not, is there a mechanism for at least preserving data as of the time a request for information is made?

VII. Modification of Records

Healthcare providers have an ingrained view that record modifications include lines through incorrect information, with new information inserted with a date and explanation. This approach, however, probably is based upon risk management advice, not a particular statute. Further, some computer software, of course, do not allow this or simply show when changes were made and who made them.

When records are updated, they are "changed" in a broad sense. Computers also make it easier to "delete" and replace than supplement any erroneous notes. Information also may be aggregated or distilled for management or financial reports. Therefore, in light of the need for modifications and corrections, plus the diversity of formats and locations of records, it makes sense to recognize the need for modifications and have a policy to address them.

VIII. Duration of Storage and Record Destruction

Standard criteria, although often confusing, dictate how long to save paper records, depending upon reasons for keeping the records. These standards become clouded in determining applicable regulatory provisions, e.g., income tax codes and statute of limitations. It is worthwhile to have a single document that outlines these policies, and lawyers are valuable advisors in creating such policies.

Although a common instinct is to think that all records should be kept for as long as possible, it simply is not possible to do so. Further, elimination of paper records saves a significant amount of space. Electronic records can be stored more easily but still have to be stored on some type of media in some type of location, and storage of digital media may require back-ups. Even modern media may become obsolete and difficult to "read." Many types of records (e.g., telephone records, voicemails, and emails) often are deleted or the substance of such information is preserved in other ways. Finally, if records are supposed to be maintained, then they have to be produced when requested and relevant, in litigation, and providers can be penalized if the records are irretrievable. On the other hand, records that are legitimately destroyed pursuant to an existing document destruction policy are less likely to create difficulties.

As everyone knows, records purportedly deleted may be retrievable by technical wizards, like Kroll OnTrack. This is costly, however. Therefore, it makes more sense to know which records need to be maintained and for how long.

IX. Don't Let "The Perfect" Be the Enemy of "The Good"

Many other issues can arise. Lawyers have to appreciate the unique characteristics—and limitations—of the businesses they advise. Prevention—like insurance—needs to be practical and cost effective. Hopefully, the foregoing outline is at least a start toward these goals.

** This article is reprinted with the permission of the Connecticut Law Tribune.*

Editor's Corner

A New Year . . . A Look to the Future

Rebecca L. Williams, RN, JD
Davis Wright Tremaine LLP
Seattle, Washington

A new year invites both looking back on where we have been and looking ahead to what may lie in store. Much has happened last year in the realm of health information and technology. And we can expect many developments and changes in the new year. This issue of *HIT News* touches on some of the developments we may be wrestling with in the coming year. . . or years.

Taking a proactive approach to dealing with information in litigation, particularly electronic discovery, James Rosenblum begins this issue of *HIT News* with practical strategies for smaller providers in "Preparing for Litigation—Before It Strikes."

We then move to HIPAA and beyond. We all know HIPAA does not specifically authorize a private right of action; however, Angela Oren raises the specter of HIPAA in tort litigation in "HIPAA Enforcement by Tort—Now It's Personal."

Next, is our Affinity Group Spotlight on our Privacy and Security Compliance and Enforcement Affinity Group. In this feature, Jenifer Belt addresses HIPAA enforcement implications in "He's Not a Doctor but He Played One on TV: HIPAA Privacy Lessons Learned (by Hospitals and OCR) from George Clooney."

Is HIPAA only a stepping stone for more expansive privacy and security restrictions on health information? Sarah Bhagwandin and Jason Froggatt explore one possibility on the horizon in "Health Information Privacy and Security Act: The Principles of the HIPAA Privacy and Security Rules Shift into Overdrive."

We wish all HIT Practice Group members a happy and healthy new year.