

# HIT News

## Preparing for Litigation— Before It Strikes\*

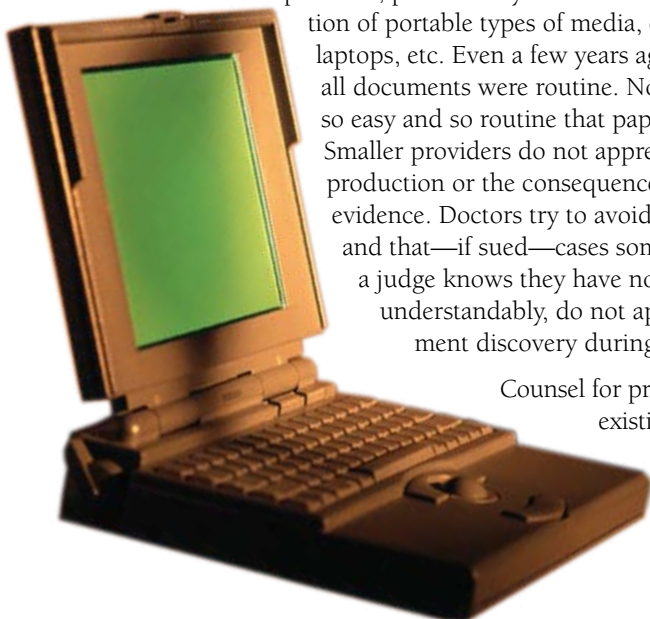
*James Rosenblum, Esquire*  
*Rosenblum Newfield LLC*  
*Stamford, Connecticut*

### 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 vendors 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

Preparing for Litigation— Before It Strikes <i>James Rosenblum, Esq.</i> .....	1
Editor’s Corner <i>Rebecca Williams, RN, JD</i> .....	3
HIPAA Enforcement by Tort— Now It’s Personal <i>Angela Oren, Esq.</i> .....	4
Chair’s Corner <i>Edward Shay, Esq.</i> .....	5
He’s Not a Doctor but He Played One on TV: HIPAA Privacy Lessons Learned (by Hospitals and OCR) from George Clooney <i>Jenifer Belt, Esq.</i> .....	6
Health Information Privacy and Security Act: The Principles of the HIPAA Privacy and Security Rules Shift Into Overdrive <i>Sarah Bhagwandin, Esq., and Jason Froggatt, Esq.</i> .....	9

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.



## 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.

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

## HIPAA Enforcement by Tort—Now It's Personal

Angela Oren, Esquire  
New Haven, Connecticut

Back in the summer of 2006, it was widely reported that the Department of Health and Human Services' Office for Civil Rights (OCR) had not levied a single civil money penalty for violation of the privacy standards,<sup>1</sup> despite having received nearly 20,000 complaints, of which over 70% were resolved. Privacy advocates expressed disappointment while some commentators took the opportunity to relegate the Health Insurance Portability and Accountability Act (HIPAA) to a regulatory back burner.<sup>2</sup>

Ironically, at about the same time that these enforcement statistics were being heralded by OCR, state appeals courts in Utah and North Carolina held that a violation of HIPAA privacy or security standards might give rise to tort liability. So while there are yet few reported cases involving HIPAA violations, the past four years of relatively quiet federal privacy and security enforcement should by no means be taken as a sign that the regulation is a paper tiger.

The Utah case, *Sorensen v. Barbuto*,<sup>3</sup> revolves around a personal injury claim against an insurance company. The plaintiff, Sorensen, who was injured in an auto accident, learned that Barbuto, his former doctor, had communicated *ex parte* with defense counsel and planned to testify on behalf of the insurer at trial. After prevailing in the personal injury claim, Sorensen sued Dr. Barbuto alleging (along with breach of contract, invasion of privacy, and intentional infliction of emotional distress) breach of professional duty based on the unauthorized disclosure of Sorensen's health information. The trial court granted Barbuto's motion to dismiss and the plaintiff appealed.

Although Sorensen's theory does not rely on the HIPAA privacy standards, Barbuto argued in his motion to dismiss that HIPAA is a bar to tort liability because it contains no private right of action. In remanding the negligence claim, the appellate court quickly dispensed with that argument by noting that the plaintiff cites HIPAA (along with other authorities including the Hippocratic Oath) not as the law that entitles the plaintiff to relief, but as the standard establishing the covered physician's professional duty. The court did not, however, address the preemption issue presented by the defendant's reliance on an exception to the state's physician-patient privilege. The defendant appealed to the Utah Supreme Court, where a decision is pending.<sup>4</sup>

*Byrum v. Acosta*,<sup>5</sup> the North Carolina case, features soap opera-like treachery involving two physician practices using a common electronic record repository. The plaintiff, Acosta, a former patient and employee of a clinic, learned that her former supervisor had used the password of Dr. Faber, the physician-owner of the clinic, to access Acosta's medical and psychiatric records on an electronic health record exchange maintained by a regional health system.

The plaintiff also discovered that her estranged mother-in-law and the mother-in-law's employer (a nearby pediatrician whose practice has no relationship to the plaintiff) had gained access, through the same database, to her records.

Characterizing the alleged acts as HIPAA violations, the plaintiff sued her former supervisor (who later went to work for the law firm representing the plaintiff's ex-husband in a custody dispute) along with her ex-mother-in-law and her employer, under various tort theories. She also sued Dr.

Faber for negligent infliction of emotional distress based on violations of HIPAA and of the user access policy for the record repository.

Faber cited HIPAA as a bar to private recovery. The trial court granted Faber's motion to dismiss for failure to state a claim. In reversing the trial court, the appeals court held that the defendant's failure to meet his obligations as a HIPAA-covered entity could be the basis for a negligence claim.

Faber also attacked the sufficiency of the complaint, arguing that it did not conform to the special rules of pleading that apply in medical malpractice cases. The court declined to characterize the cause of action as malpractice, holding that the physician's exercise of his professional judgment did not inform his acts or omissions. Instead, Faber's conduct should be judged under an ordinary negligence standard.

Substantial verdicts in cases like *Sorensen* and *Acosta*, coupled with a precipitous drive towards the adoption of electronic health information exchanges, just might open the floodgates for HIPAA-based private litigation. So what are the practical implications? The effects of such substantial verdicts may include:

- **Increased Litigation.** Substantial verdicts in cases like *Sorensen* and *Acosta* just might open the floodgates for HIPAA-based private litigation. Practitioners in states that recognize common-law torts such as invasion of privacy, public disclosure of private facts, false light, or negligent or intentional infliction of emotional distress could be vulnerable.
- **Health Information Exchange.** Community-wide health information networks as well as regional health information organizations and other health information exchanges that are or include covered entities



should consider potential tort liability when designing the architecture for the exchange and when drafting or revising user agreements.

- **Sensitive Information.** Providers who participate in health information exchanges, particularly those who generate records relating to sensitive matter such as HIV status, sexually active minors, substance abuse treatment, or mental health treatment, should carefully consider the electronic, procedural, and technical

safeguards in place to prevent unauthorized access to the information that they create, in light of both HIPAA and relevant state laws.

- 1 Rob Stein, *Medical Privacy Law Nets No Fines*, WASH POST, June 5, 2006, at A1.
- 2 See, e.g., Bob Sullivan, *Health Care Privacy Law: All Bark, No Bite?* (last visited Nov. 12, 2007), [http://redtape.msnbc.com/2006/10/two\\_years\\_ago\\_w.html](http://redtape.msnbc.com/2006/10/two_years_ago_w.html).
- 3 143 P.3d 295 (Utah Ct. App. 2006).
- 4 150 P.3d 544 (Utah 2006) (granting cert.).
- 5 638 S.E.2d 246 (N.C. Ct. App. 2006).

## Chair's Corner: HIT and the Butterfly Effect

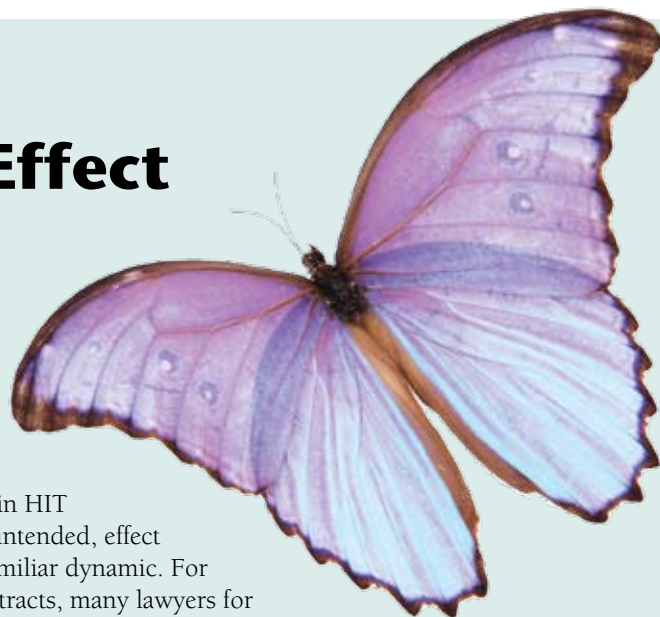
Edward F. Shay, Esquire  
Post & Schell PC  
Philadelphia, Pennsylvania

As HIT enters the 2008 calendar year, I am intrigued by the process of change in the health information technology field and how it sometimes results in the “butterfly effect,” where one small change may lead to subsequent major, and often unintended, consequences. For many of us whose first involvement in HIT came through the HIPAA Privacy Rule, the cause and, sometimes unintended, effect that links a policy change to downstream outcomes is becoming a familiar dynamic. For example, when the Privacy Rule first required business associate contracts, many lawyers for the first time got a look at the incredibly varied uses of protected health information and all of the issues that went along with some of those uses.

As HIT evolves, that change dynamic continues. The current wave of change is driven by the sometimes subtle interplay between new technologies and resulting informational developments. There is a type of “butterfly effect” that comes from digitized information that becomes available with new health information technology. For example, with the standardization of HIPAA claims formats in 2000 and the more recent mandate for NPIs, claims data has become significantly more robust and provider specific. And, because the recent decision in *Consumers' Checkbook, Center For The Study Of Services v. DHHS* has made Medicare claims data available, an information shockwave in the form of provider profiling and other inventive methods from mining claims data may be inevitable.

We can take that same nonlinear dynamic and imagine it applied to e-prescribing and electronic health records (EHRs). Both technologies have been given a recent policy push. EHRs are beginning to benefit from the encouragement of the safe harbor/Stark exception protecting certain EHR and e-prescribing donations. Secretary of the Department of Health and Human Services Mike Leavitt recently advocated for mandated e-prescribing on his personal blog. A Medicare mandate would not only launch e-prescribing as a technology but also likely would force the hand of many an EHR fence sitter. When I try to imagine the downstream information effects of these rapidly emerging technologies—and the quantum of digitization of information that goes with them—I find myself reading the recent decision in *IMS Health, et al. Rowe* less as a decision about a failed effort to curb pharma marketing practices and more as a blueprint about how EHR information about physician practice patterns will become widely available and used.

Of course, embedded in all of this change is a matrix of existing laws and interests that lawyers must sort out. The HIT Practice Group is seeking to evolve to keep pace with these changes. We are in the process of re-tooling one of our Affinity Groups to grapple with rapidly evolving health information applications. Like the early innings under the Privacy Rule, however, no one has all the answers and, sometimes, not even all of the facts. To keep our Practice Group fresh and on the cutting edge, we solicit your ideas, input and involvement. As with any emerging area of practice, there is little certainty but there can be significant opportunity. If you are interested, send me an email at [eshay@postschell.com](mailto:eshay@postschell.com).



## He's Not a Doctor but He Played One on TV: HIPAA Privacy Lessons Learned (by Hospitals and OCR) from George Clooney

Jenifer A. Belt, Esquire  
Shumaker Loop & Kendrick LLP  
Toledo, Ohio

It is (fortunately) a rare occasion when health blogs and tabloids report the same news; but when celebrities and medical information are involved, it is not at all surprising. In early October 2007, both types of media reported the suspension of twenty-seven hospital employees and the investigation of as many as forty workforce members following a visit by George Clooney and his girlfriend to Palisades Medical Center for treatment for injuries sustained in a motorcycle accident. The news has sparked a debate about what impact, or teeth, the Health Insurance Portability and Accountability Act (HIPAA) privacy rule has and whether the Office for Civil Rights (OCR) is doing enough to enforce the rules.

The privacy rule proposed in November 1999 and issued in final form in December 2000, then “final final” form in August 2002, took effect for most healthcare providers in April 2003. Unfortunately, the issuance of the final rules created as much confusion as clarity, leading many providers to wonder (mistakenly) how they would continue to conduct business without exchanging necessary information to facilitate care and treatment. Although the privacy rule was intended to make it much easier to share information for legitimate purposes (treatment, payment, and healthcare operations), it also was designed to make it much more difficult to “freely” exchange information for any other purpose. In reality, implementation of the rule has been a learning curve for providers, patients, and government alike. More than four years later, questions continue to arise about use of patient names, sharing information with family members and friends, sharing information with law enforcement, and other scenarios, despite that each of these have been addressed and “clarified” over the years by OCR.

### I. How Does OCR Enforce the Privacy Rule?

OCR is responsible for enforcing the HIPAA privacy rule. Its enforcement process largely is complaint driven, i.e., it investigates complaints referred to it as opposed to conducting random investigations for compliance.

OCR's authority to investigate complaints is limited to complaints that:

- Are against covered entities;



- Are registered within 180 days of the occurrence of violation or such later time as the person should have known of the violation (absent extenuating circumstances);
- Allege an action, that if true, would violate the privacy rule; and
- Are made by known individuals (i.e., not anonymous).

In addition, if disclosure of the complainant's identity is required to conduct the investigation and the complainant will not consent to such disclosure, the complaint will be dismissed.

According to the OCR website, 16,248 of the cases completed by OCR as of September 20, 2007, (more than 75% of completed cases) were closed for failure to meet the above-cited complaint requirements. Another 2,519 were investigated and no violation found, and 5,149 were resolved through investigation and enforcement. In cases involving “enforcement,” the enforcement has ranged from voluntary compliance and corrective action to resolution/agreement.

For cases that are not resolved through such efforts, OCR may impose civil money penalties. OCR's website does not report whether civil money penalties have been issued in any case.

Some cases have not been resolved at the OCR level. According to OCR, more than 412 cases have been referred to the Department of Justice for criminal investigation (less than 1%). Presum-

ably, these cases involved more serious allegations of inappropriate use or disclosure of information than those resolved at the OCR level. In the few cases prosecuted by the Department of Justice to date, criminal fines and penalties have been imposed. Another 214 cases have been referred to the Centers for Medicare and Medicaid Services (for investigation as potential security violations).

## II. What Are the Main Types of Violations?

OCR notes that the most frequent types of violations reported involve, in order of frequency:

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Uses or disclosures of more than the minimum necessary protected health information; and
- Lack of or invalid authorizations for uses and disclosures of protected health information.

Along the same lines, the allegations involved in the Clooney matter arguably fall into the first, second, and fourth categories above, depending upon the reasons for access and persons who accessed the information.

## III. Is OCR Doing Enough?

The number of privacy complaints has increased each year since the effective date of the privacy rule regulations, as have the cases in which corrective action was taken. This could be indicative of either increasing scrutiny by OCR or increased public awareness and complaints. Despite much speculation, to date, there is no definitive answer on whether OCR will step up its enforcement efforts in the wake of the Clooney matter and numerous other similar situations that routinely occur but simply do not garner the same media attention.

## IV. What Can a Healthcare Provider Expect When OCR Receives a Complaint About It?

A healthcare provider against which a privacy complaint is filed with OCR may never become aware of it, since the vast majority of cases are closed for lack of OCR “jurisdiction.” In those cases in which OCR decides to investigate, the next step often includes contact with the provider, either informally or formally by letter, identifying the nature of the complaint and the investigation, and asking the provider to respond. The requested response often will include the provider’s version of the events, knowledge of the alleged violation, remedial action taken (if any), and policies and procedures (if any) addressing the subject matter of the alleged violation.

Providers that receive such letters should not panic but should respond in a methodical and orderly fashion. So far, OCR appears to have taken a reasonable approach in its enforcement efforts. Providers that diligently adopt reasonable measures to achieve and moni-

tor compliance and take corrective measures when warranted often will receive letters closing the matter without additional obligation.

Providers that choose to ignore such letters can be subjected to the imposition of civil money penalties that must be challenged through hearing. This can be an expensive and time-consuming process.

## V. Conclusion

The Clooney story has caused several individuals inside and outside the healthcare industry to question whether OCR’s “kinder, gentler” enforcement policy is thwarting the goals of HIPAA. The other side of the debate contends that there still is much confusion over what HIPAA does and does not allow in the way of legitimate sharing of information. The challenges for healthcare providers are to understand who should and should not have access and for what purposes, and to ensure that information is available to those who need it (and only those persons) for the purposes for which it is needed (and only such purposes).

The Clooney story also has raised concern among many that the “average” individual’s rights are being violated without anyone knowing or caring about it. The privacy and security rules require healthcare providers to periodically audit whether their policies and procedures have been followed. Such audits could focus on employees who are patients, family members of employees, and other areas of higher risk. Consistent discipline in cases of such violations can serve as a deterrent to future violations. Even though George Clooney did not seem to mind the alleged inappropriate use of his records, most patients do care when their information is improperly accessed. Healthcare providers and OCR should, too.



## The Privacy and Security Compliance and Enforcement Affinity Group

**About the Privacy and Security Compliance and Enforcement Affinity Group.** The Privacy and Security Compliance and Enforcement Affinity Group keeps you up to date on HIPAA and state privacy and security compliance and enforcement issues. For example, the group tracks:

- Federal and state legislation and case law related to health information privacy and security issues;
- Federal and state breach notification laws;
- Practical advice for privacy and security officers on handling investigations and audits;
- Updates from the Office for Civil Rights, Centers for Medicare and Medicaid Services, and Department of Justice related to ongoing and completed investigations into HIPAA privacy and security complaints and audits; and
- Activities of states involved in the ongoing Health Information Security and Privacy Collaboration and the Nationwide Health Information Network efforts.

We invite you to become a member of our Affinity Group. You can enroll online at <http://tinyurl.com/23jhdt>.

**Members of the Privacy and Security Compliance and Enforcement Affinity Group.** The HIT Practice Group wishes to thank the Privacy and Security Compliance and Enforcement Affinity Group:

### Co-leaders:

Patricia A. Markus  
Robert L. Coffield

### Members:

Betty S. Adler  
Mark D. Aurand  
Debra Glickfeld Bang  
Alice J. Becker  
Elisabeth Belmont  
Jenifer A. Belt  
Stephen W. Bernstein  
Deborah Lynn Biggs  
Michael L. Blau  
Rodney L. Buck  
Patricia I. Carter  
Ellen V. Chiniara  
Kathryn R. Coburn  
Connie R. Crawford  
Michelle Wilcox DeBarge  
Gerald E. DeLoss  
Rafael Santos Del Valle  
Heidi Y. Echols  
Sloane M. Elman  
Gregory C. Ewing  
Shari J. Fagen  
Steven M. Fleisher  
Lisa M. Frenkel  
Sherry C. Furr  
Mark T. Garsombke  
Mark C. Gary  
Nancy P. Gillette  
Phyllis F. Granade  
Sandra P. Greenblatt  
Marilyn E. Hanzal  
Robert R. Harrison  
Shannon B. Hartsfield

Barry S. Herrin  
William Reece Hirsch  
Kimberly Short Kirk  
Jo-Ellyn S. Klein  
Kenneth J. Kramer  
Joyce Leahy  
Amy S. Leopard  
Elizabeth S. Lincoln  
Kevin D. Lyles  
Marilyn Lamar  
Keisha A. Lightbourne Barros  
Tracy J. Mabry  
Daniel J. McNerney, Jr.  
Timothy E. Monaghan  
Peter Mancino  
Susan A. Miller  
John P. Murdoch, II  
Donna M. Meyers  
Kirk J. Nahra  
Charles Warren Ott  
Jennifer L. Rathburn  
Nestor J. Rivera  
Susan O. Scheutzow  
Jeffrey M. Sconyers  
Edward F. Shay  
Jeffrey W. Short  
Howard L. Sollins  
Mark Tatelbaum  
P. David Vinocur  
G. W. Taylor  
Elizabeth S. Warren  
Nancy M. Weinman  
Leigh A. Wilkinson  
Patricia Kane Williams  
Cynthia F. Wisner  
Colin J. Zick

# Health Information Privacy and Security Act: The Principles of the HIPAA Privacy and Security Rules Shift Into Overdrive

*Sarah L. Bhagwandin, Esquire,  
and Jason Froggatt, Esquire  
Davis Wright Tremaine LLP  
Seattle, Washington*

In a striking attempt to bolster patient control over the use and disclosure of personal health information, Senators Patrick Leahy (D-VT) and Edward M. Kennedy (D-MA) introduced the Health Information Privacy and Security Act of 2007 (HIPSA) (S.1814) to the Senate in July 2007. HIPSA, if passed, would extend federal privacy and security protection of health information found in the Health Insurance Portability and Accountability Act (HIPAA) beyond the healthcare system and into *any* use of health information in the economy. This legislation, which attempts to regulate any use or disclosure of health information, would impose a whole new structure of enforcement in the form of regulations and multiple layers of government oversight. It significantly elevates the role of patient discretion over health information—arguably at the expense of the efficient delivery of healthcare.

The Standards for Privacy of Individually Identifiable Health Information (known as the Privacy Rule) 65 Fed. Reg. 82596 (December 28, 2000) established the first set of national standards protecting the privacy of personal health information. The Security Standards for Protecting Electronic Protected Health Information (the Security Rule) 68 Fed. Reg. 8333 (February 20, 2003) followed with processes to protect the security of personal health information. HIPAA brought the ordinary flow of health information in the healthcare system into focus by creating a framework for defining ordinary and necessary uses and disclosures. These ordinary uses were characterized by HIPAA as uses for treatment, payment, or healthcare operations. Any use of information for treatment, payment, or healthcare operations generally was permitted under HIPAA as long as the covered entity adopted appropriate safeguards, provided individuals with a notice of their rights regarding their information, and followed the minimum necessary rule (for payment and healthcare operations).

Although HIPSA generally adopts the framework created by the Privacy Rule and the Security Rule for permissive uses and disclosures of protected health information, it departs from the rules established under HIPAA in many important ways. First, the proposed law, if enacted in its present form, creates significant new rights for individual patients and new obligations of covered entities toward individuals. Second, HIPSA creates a different

enforcement regime that would raise the stakes for properly complying with the new privacy rules. Finally, it expands the scope of entities that must comply with the new privacy rules.

## I. New Patient Rights

Individuals were given federally protected access to and rights over their health information for the first time under HIPAA. Specifically, HIPAA requires that covered entities disclose to individuals how their health information would be used in the form of a Notice of Privacy Practices, along with providing individuals with a right to: review their health information; request restrictions on uses and disclosures of their health information; amend or correct their health information; and receive an accounting of any uses or disclosures that are not for treatment, payment, or healthcare operations.

Although HIPSA adopts all of these standards, it creates a new set of requirements for covered entities that take patient rights to a whole new level. If passed, as currently proposed, HIPSA would create the following new patient rights by requiring that covered entities:

- Obtain patients' written authorization for any use or disclosure of their personal health information, including uses for treatment, payment, and healthcare operations.



- Provide patients with an opportunity to “opt out” of a covered entity’s electronic system.
- Prohibit covered entities from disclosing protected health information until the patient has had the opportunity to opt-out of any health information networks in which the receiving agent participates.
- Notify an individual when data corruption or loss of health information is discovered, whatever the source or nature of the loss.
- Notify an individual within fifteen business days of a discovery of a breach.

In addition, HIPSA provides for a private cause of action for an individual whose rights have been knowingly or negligently violated to bring a civil action.

Whereas the privacy rights established under HIPAA recognized the complexities of the healthcare system by imposing a minimal burden on ordinary uses of health information, HIPSA would encumber even routine uses by requiring written individual authorization for the most ordinary purpose.

In addition, HIPSA’s notification rules impose significant new burdens on covered entities in the event of a breach or technological breakdown. HIPAA requires covered entities to mitigate the harmful effect of “an improper or unauthorized use or disclosure.” HIPAA does not, however, specifically require that individuals be notified of a breach, although in many instances that is a necessary step for “mitigating the harm.”

In contrast, HIPSA not only specifically requires that a covered entity notify an individual in the event of a breach, it imposes a fifteen-business-day time frame from the date of discovery for the notification. As currently drafted, there is no “reasonableness” standard or any factor, other than the needs of law enforcement, that would allow an entity to delay notification of individuals.

Not only is the fifteen-business-day deadline arbitrary, in many cases, it would result in premature notification of a breach. Important questions about the scope or cause of a breach may remain unanswered even three weeks after the initial discovery. By requiring an entity to notify individuals without regard for whether the entity has been able to successfully investigate, HIPSA threatens to make already sensitive situations completely unwieldy. The potential cost to entities in good will and resources for notifications that may be too broad or not adequately supported by information could be quite high.

Further, HIPSA requires notification of individuals in the event that systems with health information are compromised in any way. Not only does this raise the temperature on even minor technological failures, it raises the stakes for entities because HIPSA provides for a private cause of action for individuals.

## II. New Enforcement Scheme

HIPSA creates an enforcement scheme that radically changes the “compliance climate” surrounding the privacy and security of protected health information. Privacy Rule and Security Rule compliance has been characterized as somewhat voluntary, mo-

tivated by a “carrot-oriented” scheme. In contrast, HIPSA would change the tone of compliance by creating a new office, delegating enforcement on the federal and state level, and creating a private cause of action—in short, creating a “stick-oriented” scheme.

### A. Office of Health Information Privacy

HIPSA creates a new Office of Health Information Privacy of the Department of Health and Human Services. This office would be charged with two purposes: conducting investigations of complaints and alleged violations, as well as conducting audits and establishing guidelines for compliance under HIPSA; and establishing and implementing federal standards and product certifications for health information technology products that handle protected health information.

HIPSA strengthens the audit capabilities of the government by creating a new office that evidently would be monitoring uses through the entire economy, not just in the healthcare system.

Further, the legislation significantly expands the scope of government oversight by requiring new standards and certifications for technology that uses health information. This provision takes privacy of information into a whole new playing field: information technology product development. As drafted, regulations potentially could govern product development throughout the economy, not just in the healthcare sector.

### B. Enforcement by Attorneys General

HIPSA delegates the enforcement of certain privacy rights to both the U.S. Attorney General and to the states’ Attorneys General.

The proposed legislation would enforce HIPSA by empowering the U.S. Attorney General to withhold federal funds from entities that fail to comply with HIPSA and by empowering the Attorney General to impose civil penalties. Specifically, HIPSA directs the U.S. Attorney General to produce regulations and procedures that debar health industry entities from receiving federal funds if they are found guilty of wrongful disclosure of protected health information. Further, HIPSA provides a schedule of civil penalties and empowers the U.S. Attorney General to assess civil penalties against health industry entities for illegal disclosure of health information or attempts to conceal such a disclosure.

In addition to rules relating to the U.S. Attorney General, HIPSA authorizes a state Attorney General to bring a civil action against an entity for violations of HIPSA that threaten or adversely affect an interest of state residents. The state Attorney General may impose civil penalties.

#### a. Civil and Criminal Penalties

As with HIPAA, HIPSA has a range of civil and criminal penalties. HIPSA allows the U.S. Attorney General to bring suit to impose the civil penalties within a six-year statute of limitation.

#### b. Private Cause of Action

Finally, in a dramatic departure from HIPAA, HIPSA creates a private right of action for individuals. Under HIPSA, an individual may bring a civil suit if his or her rights under HIPSA have been knowingly or negligently violated. The civil action can seek

preliminary and equitable relief, the greater of compensatory damages or liquidated damages of \$5,000, punitive damages (if warranted), and attorney fees.

Providing individuals with a private right to action, coupled with the notification requirements under HIPSA, significantly raises the stakes for complying with federal privacy and security rules for health information. No longer will enforcement of privacy and security laws be a matter left to government entities. Under HIPSA, individuals would be empowered to seek enforcement of the rules when they perceive a breach. If passed, this provision is likely to generate a whole new genre of litigation relating to protecting personal health information.

### **C. Who Must Comply? “Covered Entities” and By the Way, Anyone Else . . .**

The Privacy Rule and Security Rule apply to “covered entities,” which is defined as healthcare providers, health plans, healthcare clearinghouses, and sponsors of Medicare prescription drug cards. HIPSA, on the other hand, would apply to “employers, health plans, health insurers, healthcare providers and others seeking to disclose protected health information.” In other words, any entity that uses or discloses protected health information would have to comply with HIPSA.

The scope of entities covered by HIPSA undoubtedly will create significant complications for enforcing the rules. It may help clarify at least one compliance area under HIPAA: the applicability of the rules to “health plans.” Applying the Privacy Rule and Security Rule to health plans has been challenging for several reasons. For one, it has been difficult for employers as the sponsor of a group health plan to understand how their role fits conceptually under HIPAA. For some plans, it has been hard to determine how an insurer may be distinct from a group health plan for certain compliance purposes. Further, limiting HIPAA to health plans when often the same health information is available to an employer for disability and life insurance plans has seemed arbitrary.

Although HIPSA untangles these concepts by specifying that “employers, health plans, health insurers, healthcare providers and others seeking to disclose protected health information” must comply with the new rules, the expanded list of covered entities raises a number of questions. How broad is the universe of entities that would fall into the category of “others seeking to disclose protected health information”? The proposed scope of HIPSA, if left unchanged, would make the application of the rule quite unwieldy. It would take the current focus on the use and disclosure of protected health information in the healthcare industry into any use of health information.

### **D. Now What?**

Any entity doing business that uses individual health information in any way should stay tuned. Although HIPSA, with its current, broad approach, may not be enacted, a modified version or similar legislation may be coming. HIPSA, if passed, or its progeny, could be a brave new world in the area of government protection of the privacy of personal health information.

## **Health Information and Technology Practice Group Leadership**

### **Edward F. Shay**

Chair  
Post & Schell PC  
Four Penn Center Plaza  
1600 JFK Blvd  
Philadelphia, PA 19103  
(215) 587-1151 • [eshay@postschell.com](mailto:eshay@postschell.com)

### **Gerald “Jud” E. DeLoss**

Vice Chair – Membership  
Gray Plant Mooty  
500 IDS Center  
80 South Eighth Street  
Minneapolis, MN 55402  
(612) 632-3389 • [gerald.deloss@gpmlaw.com](mailto:gerald.deloss@gpmlaw.com)

### **Phyllis F. Granade**

Vice Chair – Educational Programs  
Carlton Fields PA  
1201 West Peachtree Street, Suite 3000  
Atlanta, GA 30309  
(404) 815-2701 • [pgranade@carltonfields.com](mailto:pgranade@carltonfields.com)

### **Rebecca L. Williams**

Vice Chair – Publications & Editor  
Davis Wright Tremaine LLP  
1201 Third Avenue  
Seattle, WA 98101  
(206) 757-8171 • [beckywilliams@dwt.com](mailto:beckywilliams@dwt.com)

### **Robert Q. Wilson**

Vice Chair – Research & Website  
The Bogatin Law Firm PLC  
1661 International Place Drive, Suite 300  
Memphis, TN 38120  
(901) 474-6164 • [rwilson@bogatin.com](mailto:rwilson@bogatin.com)

## **Practice Groups Staff**

### **Trinita Robinson**

Vice President of Practice Groups  
(202) 833-6943  
[trobinson@healthlawyers.org](mailto:trobinson@healthlawyers.org)

### **Emilee Simmons**

Practice Groups Manager  
(202) 833-0776  
[esimmons@healthlawyers.org](mailto:esimmons@healthlawyers.org)

### **Magdalena Wencel**

Practice Groups Coordinator  
(202) 833-0769  
[mwencel@healthlawyers.org](mailto:mwencel@healthlawyers.org)

### **Kristina Hilton**

Practice Groups Assistant  
(202) 833-0765  
[khilton@healthlawyers.org](mailto:khilton@healthlawyers.org)

## Teleconference CD Recordings – A Great Addition to Your Resource Library!

Practice Group sponsored teleconferences are held throughout the year on hot topics and analyses of healthcare law related issues and cases. If you are unable to participate in any given teleconference, you may purchase a CD recording (includes materials) by calling our Member Service Center at (202) 833-0766, or online at [www.healthlawyers.org/teleconferenceCDs](http://www.healthlawyers.org/teleconferenceCDs).

Check out our **2008 Sale** on all teleconference recordings (ends on **February 29, 2008**).

To view a listing of available CDs, please visit:  
[www.healthlawyers.org/teleconferences/CDs](http://www.healthlawyers.org/teleconferences/CDs)

For more information about future teleconferences, visit [www.healthlawyers.org/teleconferences](http://www.healthlawyers.org/teleconferences).



1025 Connecticut Avenue, NW  
Suite 600  
Washington, DC 20036-5405