

***Managing your privacy and security
compliance efforts – Hot topics for 2007***

Kirk J. Nahra
Wiley Rein LLP
Washington, D.C.
202.719.7335
KNahra@wileyrein.com

(HCCA April 2007)

Wiley Rein LLP

Hot Topics

- Primary hot topics on privacy and security for the health care industry
- Be aware of the major areas of emphasis and change
- Understand the variety of laws – much more beyond HIPAA
- What's on the horizon in hot issues

Wiley Rein LLP

1. Enforcement

- Still zip
- Will this be changing?
- How much does the enforcement approach matter?
- What does this lack of enforcement mean for you?

Wiley Rein LLP

Enforcement Statistics

- Almost 20,000 complaints
- Is this a big or small number?
- More than 73% closed
- More than 250 complaints referred to DOJ for criminal investigation
- "Our first approach to dealing with any complaint is to work for voluntary compliance. So far it's worked out pretty well." - Office of Civil Rights Head

Wiley Rein LLP

Enforcement- Opinions

- Washington Post, front page, lead story
- Headline – “Medical Privacy Law Nets No Fines, Lax Enforcement Puts Patients' Files At Risk, Critics Say”
- Lead sentence - “In the three years since Americans gained federal protection for their private medical information, the Bush administration has received thousands of complaints alleging violations but has not imposed a single civil fine and has prosecuted just two criminal cases.”

Wiley Rein LLP

Enforcement - Issues

- Is the lack of visible enforcement an actual problem?
- Are people in the health care industry ignoring the law?
- Is the “problem” a lack of enforcement or the scope of the law itself?
- What are you doing to guard against “HIPAA-creep” – a lessening of standards related to a lack of enforcement?

Wiley Rein LLP

The DOJ Enforcement Opinion

- What does it say?
 - Criminal prosecutions generally are limited to covered entities
 - DOJ Interpretation of the HIPAA Statute
 - In certain situations, "the criminal liability of the entity has been attributed to individuals in managerial roles, including, at times, to individuals with no direct involvement in the offense."

Wiley Rein LLP

Post DOJ Memo

- Several HIPAA criminal cases
- All involving employees of covered entities
- Not clear how these are being prosecuted
- All involve really bad behavior – activities that are clearly criminal, through HIPAA or otherwise
- Are these cases useful to maintain a compliance approach? Probably not. No one needs to be told they can't steal PHI for their own personal financial gain.
- Will the new Congress revisit these issues?

Wiley Rein LLP

2. Security breaches

- Perhaps the hottest issue today
- Issues within the health care industry and more broadly
- Much more than HIPAA must be considered
- Very interesting enforcement issues

Wiley Rein LLP

Security of Medical Data

- A sampling of the problems with medical data
- Humana
- Aetna
- BCBS North Carolina
- Allina
- Kaiser Permanente

Wiley Rein LLP

Medical Data

- Deaconness Hospital (first of 2007)
- Geisinger Health Systems
- Medco
- Cleveland Clinic
- Swedish Hospital
- Akron Children's Hospital
- Labcorp

Wiley Rein LLP

Medical Data

- HCA
- Georgetown University Hospital
- American Red Cross
- BCBS Florida

Wiley Rein LLP

Enforcement issues on security

- Medicare Part D issues – Led to system wide publication of new material on security risks and importance of security procedures and audits
- North Dakota Insurance Commissioner – threatened license issues with Humana after failure to notify his office of security breach issues (even though these appeared to be all Medicare issues)
- Providence Hospital System – Oregon AG
- Who else will get in the game (e.g., the FTC – remember the Eli Lilly case)

Wiley Rein LLP

CMS Guidance

- Recent CMS Guidance on portable media and PHI (laptops, PDAs, etc.)
- What is the effect of this guidance?
- Can CMS define through guidance what is reasonable under the Security Rule?

Wiley Rein LLP

Security Conclusions

- Realistic enforcement concerns, from a variety of directions
- Are you adjusting to developments involving other companies (laptops, use of public computers, encryption, two-factor authentication)
- Do you need CMS guidance to tell you that you need to give some more thought to how you are protecting your laptops?
- Requires a serious ongoing effort to stay at or ahead of the curve

Wiley Rein LLP

3. Notification and mitigation

- Important new element to the security/privacy breach debate
- Astonishing number of media reports about large and small security breaches, almost daily occurrences, affecting all industries
- Has led to state laws – in more than 35 states – about notification of individuals in the event of a security breach
- Likelihood of new federal legislation

Wiley Rein LLP

Intersection between HIPAA and state notice laws

- Security Incident
- State notice laws
- Overlaps, under and over inclusive – some “security incidents” do not require notice under state laws, some situations require notice under state laws, but not HIPAA (employee data)

Wiley Rein LLP

“Security Incident”

- HIPAA Definition – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- If there is a security incident, what happens?
- Reporting to – covered entities (by business associates)? Regulators? Individuals?

Wiley Rein LLP

Mitigation

- Mitigation involves:
 - Identifying the problem
 - Determining the cause of the problem
 - Evaluating any potential harm from the problem
 - Stopping the bleeding from the problem
 - Evaluating appropriate changes (if any)
 - Determining any other legally required steps (or appropriate business steps)
 - Does mitigation require notification to patients (if so, notice may be required even though the security and privacy rules don't talk about notice)

Wiley Rein LLP

How state law “notification” works

- Defining the incident – what happened, what information was involved
- Was there any realistic harm of harm?
- What are your contractual obligations?
- What are your legal obligations?

Wiley Rein LLP

Key Notice Issues

- What data?
- Encrypted?
- Electronic or other?
- What kind of notice standard in the relevant law(s)?
- What states are involved?
- Likelihood or risk of harm (remember, complying with the notice statute doesn't mean you won't get sued)
- Business environment?
- Consumer attitudes – what do they expect?

Wiley Rein LLP

Vendor issues on security and notification

- Overall oversight of vendors – legal responsibilities and practical obligations
- Making your contracts work for security problems – have you been updating your BA agreements to keep pace with developments?
- The vendor's role in security incidents and notification
- Can you get the right information?

Wiley Rein LLP

4. Is your privacy officer doing the right things?

- Lots of concern that lack of enforcement is affecting compliance and ongoing privacy efforts
- Much more than HIPAA to worry about
- Make sure your Privacy Officer is involved in decision-making, not just knowledge of the rules
- Some concerns with privacy officer being “downgraded”
- Relationship between privacy and security?
- H-P example

Wiley Rein LLP

5. Litigation Issues – HIPAA Workarounds

- Increasing awareness of privacy and security in litigation
- Volume of privacy-related litigation has been small, but steadily increasing
- Wide range of litigation related to security breaches and identity theft
- Large number of cases where privacy rules are “involved” – cases involving medical records, employee records, financial records, etc.
- Ongoing issue involving damages – do any exist?

Wiley Rein LLP

Private Litigation

- Colorado Hospital case
- Hospital sought to stop a media firm from publishing PHI from an internal report
- Court held that there is no private cause of action to enforce HIPAA
- HIPAA doesn't regulate media
- Isn't that obvious?
- Does it matter if its obvious?

Wiley Rein LLP

Interesting cases

- Parker v. Quinn (Miss.) – Pharmacy received reports of fraud involving pharmacists. Patient information was disclosed in connection with the investigation, and the patients sued. Good faith disclosure of information meant no 1983 claim and no invasion of privacy claim (under HIPAA or otherwise). Privacy claims were “totally without merit.”

Wiley Rein LLP

Interesting cases

- Rosales v. Bakersfield (CA) – In wrongful death case, medical records were subpoenaed. Doctor objected to production of information. Court found production was appropriate because all HIPAA steps had been met.

Wiley Rein LLP

Interesting cases

- Sorensen v. Barbuto (Utah) - Doctor provided information to defense attorneys in a case brought by the doctor's former patient. While the Court dismissed breach of contract claims against the doctor, the appeals court allowed a claim to proceed for "a breach of the physician's fiduciary duty of confidentiality."

Wiley Rein LLP

Interesting cases

- Acosta v. Bynum (N.C. Ct. App.)
- Court reinstated a claim for intentional infliction of emotional distress against a psychiatrist who allegedly allowed an officer manager access to psychiatric records that were then used to cause harm to a patient.
- The complaint references HIPAA as creating a standard of care for the defendant.
- The trial court had dismissed the claim, in part because HIPAA does not create a private cause of action.
- The appellate court reversed, not because HIPAA creates a private cause of action, but because they found it appropriate to use HIPAA as creating a standard of care in making claims that a defendant violated a standard of care.

Wiley Rein LLP

6. Litigation issues – Open Records laws

- In State ex rel. Cincinnati Enquirer v. Daniels, 2006-Ohio-1215 (Mar. 17, 2006), the Ohio Supreme Court, in dicta, indicated that the State Freedom of Information laws trumped the HIPAA Privacy Rule, so that information held by the state, to the extent it had a HIPAA covered entity role, also would be subject to disclosure under the freedom of information act.

Wiley Rein LLP

Texas Open records Decision

- Reporter requested statistical information regarding allegations of abuse and subsequent investigations of abuse in state mental facilities.
- Department refused to produce based on HIPAA
- Court assumed that information was covered by HIPAA, and that Department was a covered entity, and then said that information should be produced, because it was required by the open records law to be produced.

Wiley Rein LLP

7. Electronic health records

- Biggest privacy and security policy issue on the horizon
- Is it possible to balance the desire for electronic medical records/personal health records with appropriate privacy and security?
- Debate on EMRs/PHRs will drive a new evaluation of HIPAA

Wiley Rein LLP

Wall Street Journal

- “As the health care industry embraces electronic recordkeeping, millions of pages of old documents are being scanned into computers across the country. The goal is to make patient records more complete and readily available for diagnosis, treatment and claims-payment purposes. But the move has kindled patient concern about who might gain access to sensitive medical files – data that now can be transmitted with the click of a computer mouse.”

Wiley Rein LLP

What are the HIPAA issues?

- Who is responsible for the records -Covered entity? Business associate? Or both?
- What is the HIPAA status of the entities that oversee the records systems?
- Who is responsible for security? Individual rights?
- Who will determine access issues?
- Whose fault/responsibility is it in the event of a problem?

Wiley Rein LLP

What are the Issues (2)

- Are there entities that don't have appropriate HIPAA status?
- Do the HIPAA rules need to be changed?
- Are new rules necessary for this environment?
- How much privacy/security will be "too much?"
- Are different enforcement approaches necessary?

Wiley Rein LLP

8. Employer issues

- Connection with EMRs (new initiatives from employer and insurance groups)
- New Initiatives
- Wellness programs
- Overall involvement in cost control
- Harder and harder to draw lines between covered entities and employers

Wiley Rein LLP

9. Politics

- Criticism of existing HIPAA enforcement
- Recognition of “gaps” in HIPAA – areas where “health care information” is not sufficiently protected
- Pressure on EHR/PHR systems and recognition of prominent role of non-covered entities and business associates
- Is this a perfect storm for new legislation?

Wiley Rein LLP

10. Medical Identity Theft

- Major study (May 2006)
<http://www.worldprivacyforum.org/medicalidentitytheft.html>.
- Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information -- without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods.
- Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name

Wiley Rein LLP

World Privacy Forum Report

- Aside from normal elements of fraud, victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them.
- Medical identity theft is largely a crime that is perpetrated by trusted insiders.

Wiley Rein LLP

The Cleveland Clinic Case

- Makes the connection between identity theft and health care fraud
- Indictment of a former Cleveland Clinic Florida employee for conspiracy to commit health care fraud with personal information of more than 1,100 Naples patients
- Patient information provided to outsider, who then fabricated Medicare claims

Wiley Rein LLP

Conclusions

- Privacy and security remain hot topics
- Enforcement likely to increase somewhat – but major threat may not come from HHS
- New Congress may change the debate on privacy and security
- Increased likelihood of new legislation – to expand HIPAA to currently non-covered entities, or alter the focus of attention for privacy in the health care industry

Wiley Rein LLP