Top Privacy and Security Developments for the Health Care Industry

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

(December 13, 2007)

Hot Topics

- Hit some of the highlights of hot topics in HIPAA, Gramm-Leach-Bliley and State Law for the Health Care industry
- Mainly identify some of the areas requiring new attention or a re-evaluation of what you are doing and a discussion of big issues that are on the horizon

1. Enforcement

- Short discussion - Still zip
- Will this be changing? (we've been saying it will for a long time, but no concrete developments)
- How much does the enforcement approach matter?

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?

Security enforcement

- Is a different approach coming on security?
- One very extensive audit of a hospital, which has been creating worries about pro-active security reviews
- No real basis for general conclusions that there is a new approach
- But the audit questions are VERY intimidating

2. Are we seeing cracks in the litigation wall?

- We know there is no HIPAA cause of action
- We're starting to see breach of confidentiality claims that are called things other than HIPAA
- We're starting to see HIPAA emerge as a "standard of care" that can be breached

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."

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.

3. Wellness programs

- Significant increased interest in wellness programs as a component of overall cost control
- Many new companies providing assistance with wellness programs
- Employers oversee and encourage these programs – and pay for them
- Presumably, employers will need to see a return on investment

HIPAA issues on wellness programs

- HIPAA never dealt well with disease management/wellness programs
- Didn't really consider "wellness" programs run through or by employers at all
- Enormous tensions with HIPAA rules and the overall policy that employers shouldn't be able to act on employee health care information

HIPAA issues

- Are wellness programs considered treatment?
- Are they covered by HIPAA at all?
- What if the contracts are between vendors and employers – outside of the “health plan?”
- Does it matter if there is a business associate agreement?

HIPAA issues

- Can employers provide incentives? How about penalties? What information can they have to allow these?
- What information can employers have about employees taking care of themselves?
- Big policy issue – can employers charge more for people who don't participate or don't take steps to improve their health?
- Bigger picture policy issue – is the "one price for all" model for employer sponsored health care programs going to continue to exist?

4. Off-shoring

- An increasing requirement in government programs (particularly through CMS)
- Imposition of new standards related to knowing what your vendors are doing off-shore
- While there aren't prohibitions YET, be very very careful.
- Remember – all of the controversy stems from a very small number of insignificant situations.
- Have you dealt with this in your BA contracts?

5. G-L-B Issues

- Not really an issue for health care providers
- Some new issues for insurers, for marketing and identity theft (although more tied to FCRA and FACTA)
- GLB is setting standards for some areas (mainly security)
- Not significantly more enforcement than HIPAA (but no one seems to notice)

6. 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?
- Significant likelihood that the debate on EMRs/PHRs will drive a new evaluation of HIPAA

Current status

- Lots of debate and discussion by lots of people about these very challenging issues
- But, the marketplace is moving forward without rules
- Be aware of this uncertainty as you are working with your company's electronic records activities

Balancing Interests

- Goal of widespread consumer empowerment
- Consumers need to have confidence in the system in order to use it
- Not discourage innovation
- Keep an eye on costs
- But develop rules that will permit the system to move forward
- Recognizing that the marketplace is moving forward in any event

AHIC/CPS Recommendation

All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements.

Impact

- Health care providers who are not covered entities
- PHR providers who provide services directly to patients
- RHIOs and other “networks” who play a central role
- Obligations should be met directly, rather than “just” through BA contracts

What else is happening - NCVHS?

- NCVHS raised "a significant concern . . . that many of the new entities essential to the operation of the Nationwide Health Information Network (NHIN) fall outside HIPAA's statutory definition of 'covered entity.'"
- These include a wide variety of entities who may or may not be business associates (along with a wide range of noncovered health care providers).
- NCVHS concluded that "business associate arrangements are not sufficiently robust to protect the privacy and security of all individually identifiable health information."

What else is happening – Kennedy-Leahy

- Wholesale abandonment of HIPAA environment
- Abandonment of the Office of Civil Rights as an enforcement agency, in favor of a new Office of Health Information Privacy;
- Creation of an extensive new notice requirement, including a new variety of "opt-out" rights;
- Creation of new "informed consent" procedures, even for treatment and payment uses and disclosures;

What else is happening – Kennedy-Leahy

- Requirement for authorizations for a wide variety of other disclosures (where none is required today), particularly health care operations;
- Expansion of civil and criminal penalties;
- Authorization for enforcement by State attorneys general;
- Creation of a private right of action for individuals.

What else is happening – Kennedy-Leahy

- Prospects? Prediction – slim to none
- Likely will be part of the overall debate on health care privacy
- Could result in dramatic changes to the overall health care privacy landscape
- Full employment for health care privacy officers, consultants and lawyers

7. Confusion from too many laws

- Multiplicity of laws continues to create confusion and concern
- Providers and others still reluctant to share information in situations where HIPAA permits sharing
- Is this a cop-out or real confusion?

Confusion

- Do these state laws increase protections or only increase confusion?
- Virginia Tech situation – confusion over laws led to too little action
- Part of the EMR/PHR debate also – do more laws work?
- A real policy question as to whether a single, more straightforward set of rules would work better

Conclusions

- Enforcement likely to increase somewhat – but major threat may not come from HHS
- 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
- Increased likelihood of litigation that is effective against privacy/security breaches
- Lots of big picture policy issues on the immediate horizon