

Privacy **TRACKER**

iapp

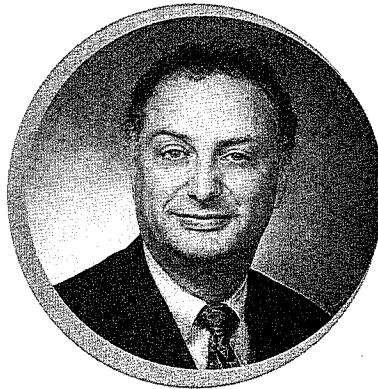
A publication from the International Association of Privacy Professionals

EMRs, PHRs, RHIOs and the New Health Care Privacy Debate

Kirk J. Nahra

While the health care industry finally seems to have settled into the HIPAA privacy and security regime, the building pressure to develop effective means of creating electronic medical records (EMR) and using health information technology (HIT) to improve health outcomes and reduce administrative costs is creating a new debate as to whether the existing privacy and security rules are reasonable and effective in today's evolving health care information environment. In fact, the marketplace for electronic medical information is moving quickly—so far, much more quickly than the evolving regulatory structure. Today, we are seeing the realistic possibility that there may be new privacy and security rules for the health care industry (and the many others who use health care information) in the near future, driven by the use of new technology to store,

See Health Care Privacy Debate, page 3



H.R. 4791: A Federal Data Breach Bill That Could Pass This Year

Thomas Oscherwitz

Out of the cluster of data breach bills pending before Congress, the bill with the best chance to advance before the end of the session may be H.R. 4791, the Federal Agency Data Protection Act.

H.R. 4791 seeks to “protect personally identifiable information of individuals that is maintained in or transmitted by Federal agency information systems.”

H.R. 4791 has the following key provisions as introduced:

- Requires federal agencies to notify consumers of breaches of personally identifiable information.
- Requires each federal agency to conduct a Privacy Impact Assessment before it enters into a contract with a “data broker” to access a “data broker” database with personally identifiable information.

See Federal Data Breach Bill, page 16



In This Issue

| | |
|---|-----------|
| EMRs, PHRs, RHIOs and the New Health Care Privacy Debate..... | 1 |
| H.R. 4791: A Federal Data Breach Bill That Could Pass This Year..... | 1 |
| Letter from the Editor..... | 2 |
| Legislative Action..... | 18 |
| Credit Agencies & ID Theft..... | 18 |
| Data Security & Breach..... | 20 |
| Government Records, SSN & Identification..... | 21 |
| Internet..... | 23 |
| Marketing..... | 23 |
| Children & Education..... | 24 |
| Financial, Insurance & Mortgages..... | 24 |
| Employment..... | 26 |
| Medical..... | 26 |
| Telecommunications & RFID..... | 27 |
| Session Calendar 2008..... | 28 |

Federal Data Breach Bill

continued from page 1

- Requires each agency to have a plan to protect agency computers and networks from risks posed by unauthorized peer-to-peer file sharing programs.
- Requires federal agencies to bring in outside auditors to review their information systems annually.

Government and private sector privacy professionals should keep this legislation in mind—despite its modest scope—because of the precedents it can set for more comprehensive federal data breach notification and data broker legislation.

Background on Federal Data Breach Laws

While more than 38 states and the District of Columbia have passed data breach laws, Congress has been slow to pass such a law—though not for a lack of trying. As early as 2003, Senator Dianne Feinstein introduced the first federal data breach bill, the Notification of Risk to Personal Data Act¹. In subsequent Congresses, at least six House and Senate committees have introduced comprehensive federal data breach bills that cover private and public sector breaches. Not one of these committee bills has made it into law.

To date, the Department of Veterans Affairs Information Security Enhancement Act of 2006 is the only data breach notification law passed by Congress. This law applies narrowly to the breach notification procedures of the Department of Veterans Affairs.

In the absence of definitive legislation from Congress, federal regulators and the Office of Management and Budget (OMB) have stepped into the breach (pun intended). Federal financial regulators have issued guidance for breach notification procedures for financial institutions. Notably, financial regulators require financial institutions to notify individuals of a data breach “if the institution determines that misuse of its information has occurred or is reasonably possible.” OMB, meanwhile, administratively established breach guidelines for federal agencies through Memorandum 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” in May 2007. This memorandum directed agencies to establish breach notification policies and set up a framework for agencies to reduce the risk of data breaches.

Why H.R. 4791 Might Move

Contrary to other data bills caught in the crosshairs of congressional jurisdictional fights, H.R. 4791 has a

narrow focus on federal agencies and has just a single committee referral to the House Committee on Oversight and Government Reform. Giving the bill even greater momentum, the bill’s sponsor, Representative William Lacy Clay, is a subcommittee chair on the Committee, and counts among his cosponsors Full Committee Chairman Henry Waxman. Representative Clay already has held a hearing on the bill.

Because the bill is confined to federal activity only, it can also avoid the contentious issue of federal preemption of state law, which has slowed down other data breach bills. Additionally, because the bill is confined to federal agencies only, there are fewer private sector and public interest constituencies with parochial interests that could slow down the bill.

H.R. 4791 has the following key provisions:

Expansive Definition of PII

H.R. 4791 would extend data breach obligations to all personally identifiable information. The bill defines “personally identifiable information” as “any information about the individual maintained by an agency including information:

- (A) about the individual’s education, finances, or medical, criminal, or employment history; or
- (B) that can be used to distinguish or trace the individual’s identity, including name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; or
- (C) that is linked or linkable to the individual.”

The bill calls for timely agency “notification to individuals whose personally identifiable information may have been compromised or accessed during such breach, based on government-wide risk categories.” These risk categories are to be defined by the Director of OMB.

Depending on how OMB defines risk categories, this bill could transform what is commonly thought of as a data breach. First, OMB could require notification for losses of PII where the individual faces no plausible risk of identity theft. In addition, notification could apply to a broad range of harms such as loss of health privacy or the publication of embarrassing facts beyond the scope of most data breach bills.

H.R. 4791’s definition of PII is far broader than the definition

of PII in most data breach notification statutes, which tend to focus on consumer names in combination with Social Security numbers, state identification numbers, or financial account numbers with PIN and pass codes, and other very sensitive personal information. This bill language is also in contrast to the White House Identity Theft Task Force Report recommendation that breach notification should “occur only when the risks to consumers are real—that is, when there is a significant risk of identity theft due to the breach.”²

Carve-Out for Encrypted Data

As with many state data breach laws, H.R. 4791 would exempt from notification requirements breaches of information security where the personal “information can reasonably be determined to be unusable by unauthorized persons.” This exception enables agencies to avoid the burdens of notification by using encryption or other technologies. From a practical perspective, this exception makes sense because a data breach shouldn’t really be considered a breach if bad actors can’t get access to the data.

Agencies Need to Complete Privacy Impact Assessments to Work with Data Brokers

Beyond its role in advancing the data breach debate, H.R. 4791 has important provisions regarding the use of private sector data by government entities. Critics of the Privacy Act of 1974 argue that the law has not kept up with the emergence of private sector databases or with the increasing federal appetite for third party data sources.

Section 8 of H.R. 4791 would require government agencies to conduct privacy impact assessments (PIAs) prior to “purchasing or subscribing for a fee to information in identifiable form from a data broker.” Privacy impact assessments are public documents that require agencies to look at the costs and risks of using new sources of personal data. A PIA typically has a description of the project, a risk assessment, an evaluation of the potential threats to privacy, and a recommendation on ways to minimize that risk.

The bill goes on to prohibit any Federal agency to sign a contract with a data broker unless the PIA is completed.

Data brokers are broadly defined by the bill to mean a “business entity that, for monetary fees or dues, regularly engages in the practice of collecting, transmitting, or providing access to sensitive information in an identifiable form on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.”

Bill Status

On March 11th, the Government Reform Committee’s Subcommittee on Information Policy, Census, and National Archives held a hearing on the data broker portion of H.R. 4791. The hearing was entitled “Privacy: The Use of Commercial Information Resellers by Federal Agencies.” Witnesses included Karen Evans, the Administrator for Electronic Government and Information Technology at OMB; Hugo Teufel III, Chief Privacy Officer of the Department of Homeland Security; and Linda Koontz, Director of Information Management Issues at the Government Accountability Office (GAO).

Based on the comments from the hearing and other public input, Committee staff are revising the bill and an updated draft is expected in April.

Mr. Oscherwitz serves as Vice President of Government Affairs and Chief Privacy Officer of ID Analytics, the leader in on-demand identity intelligence solutions. Previously, Mr. Oscherwitz worked for five years as Counsel to Senator Dianne Feinstein on the United States Senate Judiciary Committee, where he specialized in identity theft and privacy issues. Mr. Oscherwitz, a Certified Information Privacy Professional, can be reached at toscherwitz@idanalytics.com.

¹ Full disclosure – I worked on this bill as Senator Feinstein’s Judiciary counsel.

² *Combating Identity Theft: A Strategic Plan*, The President’s Identity Theft Task Force, p. 36 (April, 2007).