Update on Privacy and Security Issues for Retail Pharmacies

Introduction

This white paper addresses recent developments regarding data privacy, including data mining, enhanced enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), breach notification requirements and new HIPAA regulations.

Data Mining

Use of Physician Prescribing Information

Sorrell v. IMS Healthcare Inc., 131 S. Ct. 2653 (2011). This United States Supreme Court decision strikes down a Vermont law prohibiting the sale, disclosure and use of pharmacy records that reveal the prescribing practices of individual doctors for use in the marketing of drugs.[1] This data is frequently used by pharmaceutical companies to target physicians for detailing and other marketing activities.

Sorrell was fought over a Vermont law and has implications for other states, as well. In 2007, Vermont passed a law that prohibited pharmacies from sharing physician-specific prescribing patterns with companies that would, in turn, help brand-name drug manufacturers target their sales to those doctors. Vermont intended to protect doctors from intrusive marketing, which could drive up health care costs if doctors prescribe more expensive brand-name drugs. Maine and New Hampshire passed similar laws, but in light of the *Sorrell* decision, the Maine attorney general agreed that the Maine law should be declared unconstitutional, and the New Hampshire attorney general agreed that the *Sorrell* decision rendered the New Hampshire law unenforceable.[2]

Escalating HIPAA Compliance

First Civil Monetary Penalty Imposed for HIPAA Violations

In a February 22, 2011 press release announcing the first civil monetary penalty imposed by the US Department of Health & Human Services (HHS) for a HIPAA violation, the government announced that, despite nearly 10 years of complacency, it would be enforcing the HIPAA regulations:

> *Covered entities and business associates must uphold their responsibility … and adhere closely to all of HIPAA's requirements. The U.S. Department of Health and Human*

[1] "Act Relating to Increasing Transparency of Prescription Drug Pricing and Information," Vt. Stat. Ann. tit. 18, § 4631 (2007).

[2] Thomas R. Julin, Sorrell v. IMS Health May Doom Federal Do Not Track Acts, 10 PVLR 35 (Sept. 5, 2011).

Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules.[3]

In February 2011, HHS issued a Notice of Final Determination finding that Cignet Health of Prince George's County, Maryland violated the Privacy Rule of HIPAA. HHS imposed a civil money penalty (CMP) of $4.3 million for the violations, representing the first CMP issued by HHS for violations of the HIPAA Privacy Rule. The CMP is based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Significantly Increased CMPs

Prior to the HITECH Act, HHS was authorized to impose on any person who violates HIPAA CMPs of up to $100 per violation, not to exceed $25,000 for identical violations during a calendar year, provided that the violation was not a criminal offense, and the person otherwise liable for the penalty did not know or with reasonable diligence would not have known that the act constituted a violation. As amended by the HITECH Act and effective for violations occurring on or after November 30, 2009, the potential civil penalties for HIPAA violations have turned from what many regarded as a slap on the wrist into a potentially meaningful weapon against HIPAA violators and an important element in establishing public trust in the privacy and security of protected health information (PHI). Under the HITECH Act, the penalties for a HIPAA violation that does not constitute a criminal offense are as follows:

Violation Category	**Each Violation**	**All Identical Violations in a Calendar Year**
Did not know and by exercising reasonable diligence, would not have known of the violation	$100 to $50,000	Up to $1,500,000
Violation due to reasonable cause and not to willful neglect	$1,000 to $50,000	Up to $1,500,000
Violation due to willful neglect and **corrected** during the 30-day period the violator knew or should have known of the violation	$10,000 to $50,000	Up to $1,500,000
Violation due to willful neglect and **not corrected** during the 30-day period the violator knew or should have known of the violation	$50,000	Up to $1,500,000

Enforcement Through State Attorneys General

The HITECH Act includes another sweeping expansion of enforcement efforts – state attorneys general may commence civil actions on behalf of state residents in federal court with regard to HIPAA violations occurring after February 17, 2009, as long as no federal action has been instituted by HHS against the

[3] Press Release, Office for Civil Rights, Department of Health and Human Services, HHS Imposes a $4.3 Million Civil Money Penalty for HIPAA Privacy Rule Violations, quoting Georgina Verdugo, Director (February 22, 2011).

person with respect to the same violation. This right is in addition to any other powers that the attorney general may have under state law. A state bringing such an action must notify HHS prior to bringing the action or as soon as feasible after bringing the action, and HHS may intervene, be heard on all matters arising in the action and file petitions for appeal. The purpose for such actions may be to enjoin further HIPAA violations or obtain damages on behalf of the state's residents. Damages are low, however – up to $100 per separate violation with a maximum of $25,000 for all violations of the identical requirement in a calendar year. An award may include costs and reasonable attorney fees to the state.

During 2011, HHS conducted a series of training sessions for state attorneys general. Equipped with such training, state-level actions are anticipated.

HIPAA Privacy and Security Rule Complaint Process

The HHS Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules. One of the ways that OCR carries out this responsibility is to investigate complaints it receives. OCR may also conduct compliance reviews to determine if covered entities are in compliance. It also performs education and outreach to foster compliance with requirements of the Privacy and Security Rules.

If OCR accepts a complaint for investigation, it will notify the person who filed the complaint and the covered entity named in it. The complainant and the covered entity are then asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. Covered entities are required by law to cooperate with complaint investigations.

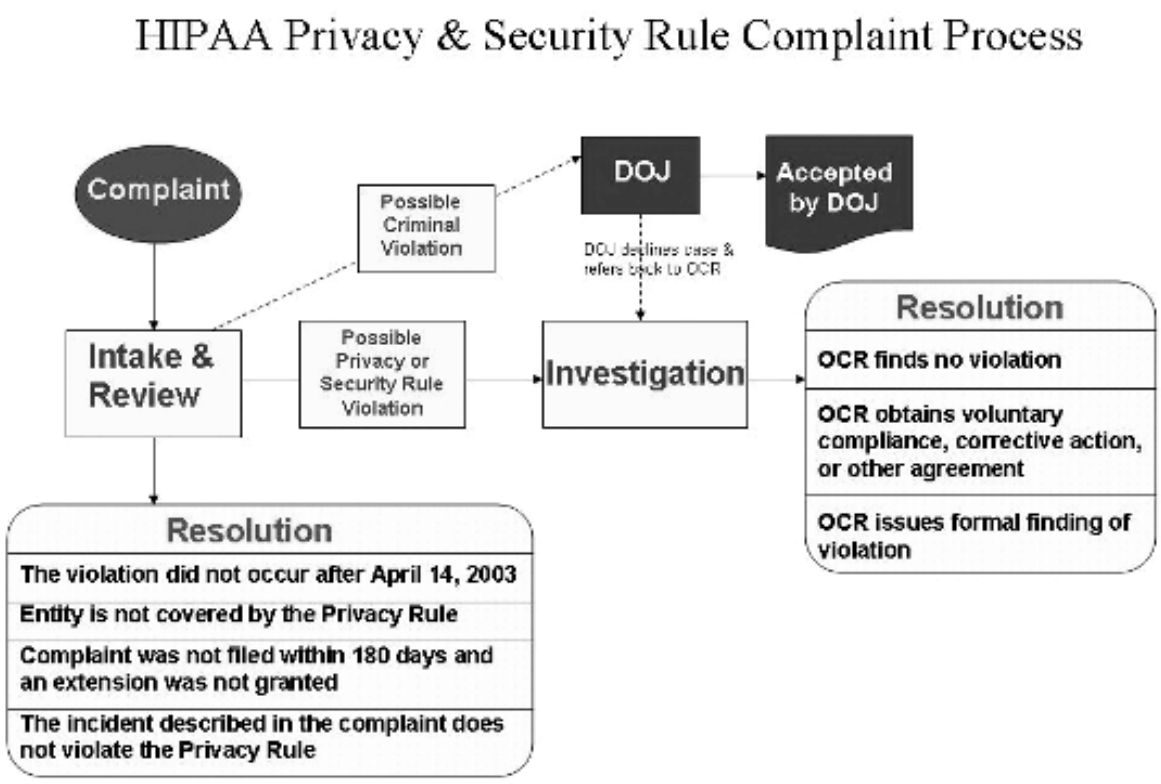
If a complaint describes an action that could be a violation of the criminal provision of HIPAA, OCR may refer the complaint to the Department of Justice for investigation.

OCR reviews the information, or evidence, that it gathers in each case. In some cases, it may determine that the covered entity did not violate the requirements of the Privacy or Security Rule. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:

- Voluntary compliance;
- Corrective action; or
- A resolution agreement.

Most Privacy and Security Rule investigations are concluded to the satisfaction of OCR through these types of resolutions. OCR notifies the person who filed the complaint and the covered entity in writing of the resolution.

If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose CMPs on the covered entity, as in the *Cignet* case described above. If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case. Complainants do not receive a portion of CMPs collected from covered entities; the penalties are deposited in the US Treasury. The follow is a diagram of the complaint process:



Source: US Department of Health & Human Services

Trends in HIPAA Enforcement Actions

The common belief that HHS does not actively enforce HIPAA does not stand up under the examination of HIPAA complaints. Figure 1 shows the trend in HIPAA complaints steadily rising from about 6,000 in the first full year of HIPAA implementation to more than 8,500 in 2010.

Figure 1

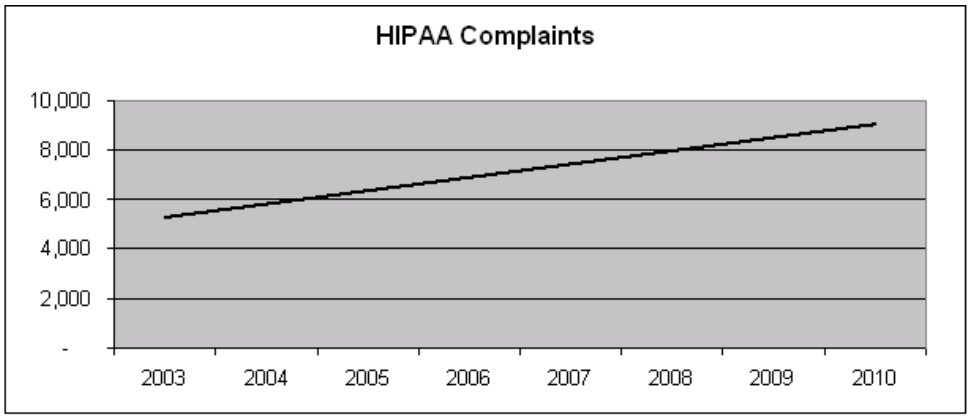
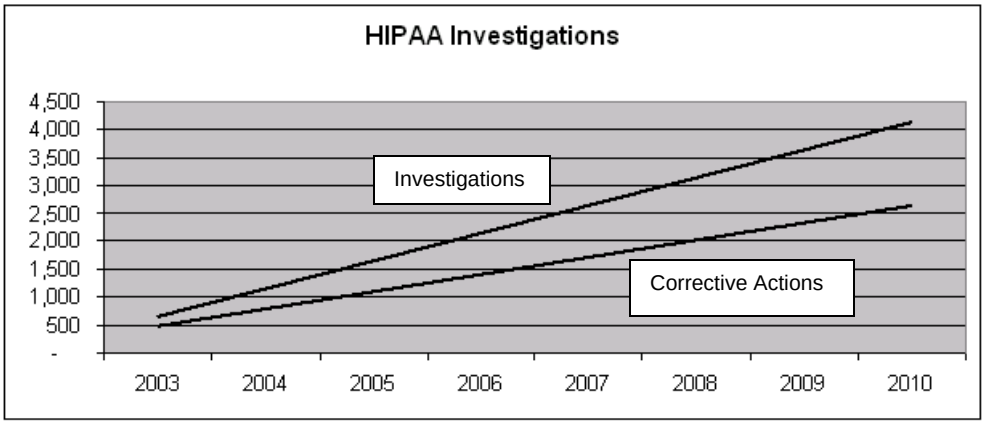


Figure 2 shows the trend in HIPAA investigations increasing from about 1,400 in the first full year of implementation to more than 4,200 in 2010, while the number of HIPAA corrective actions increased from about 1,000 to more than 2,700 during that same period.

Figure 2



With a new emphasis on enforcement, a continued increase in investigations and corrective actions is anticipated.

Examples of Retail Pharmacy HIPAA Actions

The top three issues investigated by HHS that result in corrective actions are (1) impermissible use or disclosure of PHI; (2) inadequate safeguards; and (3) failure to provide access to an individual's health records. The following are examples of HIPAA issues encounters by retail pharmacies.

1. Pharmacy Chain Enters Into Business Associate Agreement With Law Firm

Issue: Impermissible Uses and Disclosures; Business Associates

A complaint alleged that a law firm working on behalf of a pharmacy chain in an administrative proceeding impermissibly disclosed the PHI of a customer of the pharmacy chain. OCR investigated the allegation and found no evidence that the law firm had impermissibly disclosed the customer's PHI. However, the investigation revealed that the pharmacy chain and the law firm had not entered into a business associate agreement, as required by the Privacy Rule to ensure that PHI is appropriately safeguarded. Without a properly executed agreement, a covered entity may not disclose PHI to its law firm. To resolve the matter, OCR required the pharmacy chain and the law firm to enter into a business associate agreement.[4]

2. Pharmacy Chain Revises Process for Disclosures to Law Enforcement

Issue: Impermissible Uses and Disclosures

A chain pharmacy disclosed PHI to municipal law enforcement officials in a manner that did not conform to the provisions of the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required this chain to revise its national policy regarding law enforcement's access to patient PHI to comply with the Privacy Rule requirements, including that disclosures of PHI to law enforcement only be made in response to written requests from law enforcement officials, unless state law requires otherwise. The revised policy was implemented in the chains' stores nationwide.[5]

3. Pharmacy Chain Institutes New Safeguards for PHI in Pseudoephedrine Log Books

Issue: Safeguards

A grocery store-based pharmacy chain maintained pseudoephedrine log books containing PHI in a manner so that individual PHI was visible to the public at the pharmacy counter. Initially, the pharmacy chain refused to acknowledge that the log books contained PHI. OCR issued a written analysis and a demand for compliance. Among other corrective actions to resolve the specific issues in the case, OCR required that the pharmacy chain implement national policies and procedures to safeguard the log books. Moreover, the entity was required to train all staff on the revised policy. The chain acknowledged that log books contained PHI and implemented the required changes.[6]

[4] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case20

[5] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case17

[6] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case18

4. National Pharmacy Chain Extends Protections for PHI on Insurance Cards

Issue: Impermissible Uses and Disclosures; Safeguards

A pharmacy employee placed a customer's insurance card in another customer's prescription bag. The pharmacy did not consider the customer's insurance card to be PHI. OCR clarified that an individual's health insurance card meets the statutory definition of PHI and, as such, needs to be safeguarded. Among other corrective actions to resolve the specific issues in the case, the pharmacy revised its policies regarding PHI and retrained its staff. The revised policies are applicable to all individual stores in the pharmacy chain.[7]

Breach Notification

Information security experts are calling 2011 one of the worst years for data security breaches in the last 10 years. Since 2002, 46 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.[8] Alabama, Kentucky, New Mexico and South Dakota have no security breach laws.[9] In 2011, at least 14 states introduced legislation expanding the scope of laws, setting additional requirements related to notification or changing penalties for those responsible for breaches.[10]

The HITECH Act includes new provisions that amend HIPAA with regard to PHI, and other federal regulations with regard to personal health records. Under the HITECH Act, as of September 23, 2009, with a few common sense exceptions, a covered entity is required to notify the subject of a breach of unsecured PHI that causes or poses a significant risk of financial, reputational or other harm to the individual. For a breach event involving 500 or more individuals, the HITECH Act requires covered entities to notify the HHS immediately. For breach events involving less than 500 individuals, the HITECH Act provides that a covered entity may maintain a log of such breaches and annually submit the log to HHS.

Since September 23, 2009, HHS received 252 reports of breach events involving 500 or more individuals. Covered entities notified 7.8 million individuals of these breaches. The most common causes reported for these large breach events were: (1) theft; (2) intentional unauthorized access to, use or disclosure of PHI; (3) human error; and (4) loss of electronic media or paper records containing PHI.

Since September 23, 2009, HHS received 30,521 reports of breaches involving less than 500 individuals. Covered entities notified 62,000 individuals of these breaches. The most common cause reported for these smaller breach events was misdirected information such as a test results sent to the wrong patient.

---

[7] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case13

[8] National Conference of State Legislatures, available at http://www.ncsl.org/default.aspx?tabid=22295

[9] *Id.*

[10] *Id.*

New HIPAA Regulations Expected

New HIPAA regulations are expected by the end of 2011. The following chart summarizes the status of the anticipated regulations:

Rule	Type	Published in Federal Register	Effective Date	Full Compliance Date	Status
Breach Notification	Interim Final Rule	8/24/2009	9/23/2009	2/22/2010	Awaiting Final Rule
Enhanced HIPAA CMPs	Interim Final Rule	10/30/2009	11/30/2009	N/A	Awaiting Final Rule
Applications of Privacy and Security Rules to Business Associates Restrictions on Marketing Prohibition on Sale of PHI Restrictions on Disclosures to Health Plans for Out-of-Pocket Payments Access to PHI Maintained in an Electronic Form	Proposed Rule	7/14/2010	TBD	Generally 180 Days Following the Effective Date	Awaiting Final Rule
Accounting for Disclosures and Access	Proposed Rule	5/31/2011	TBD	TBD	Awaiting Final Rule
Increased Patient Access to Laboratory Reports	Proposed Rule	9/14/2011	TDB	TBD	Awaiting Final Rule

Squire Sanders will continue to monitor the proposed changes to privacy and security matters. After the new regulations are issued, pharmacies will need to revise HIPAA privacy and security policies and procedures, as well as Notice of Privacy Practices, and modify their business associate agreements to ensure compliance with the regulations. For more information, please contact David W. Grauer at david.grauer@ssd.com (+.1.614.365.2786) or Scott A. Edelstein at scott.edelstein@ssd.com (+1.202.626.6602).