HIPAA/HITECH Act Enforcement: 2003-2013

The Role of Patient Complaints
In Medical Privacy and Data Security

by
Dennis Melamed
President, Melamedia, LLC
July 2013

This white paper was independently developed, produced and issued by Melamedia, LLC

About the Author

Dennis Melamed is president of Melamedia, LLC, a regulatory affairs research firm and publisher of *Health Information Privacy/Security Alert*. He serves as an adjunct professor in the Drexel College of Medicine, where he teaches graduate courses on patient data stewardship issues and regulations governing the conduct of biomedical research.

Acknowledgements

All opinions and errors are those of the author and do not reflect the opinions or views of the professionals who graciously reviewed and made comments during the development of this white paper. The author would specifically like to thank the following individuals for their comments and suggestions:

John Christiansen, JD, Principal, Christiansen IT Law

Robert Gellman, JD, Privacy Consultant

Adam Greene, JD., MPH, Partner and Co-Chair of Health Information Practice Group, Davis Wright Tremaine LLP

Invitation to Comment

This white paper and those to follow are intended to foster an ongoing discussion of patient data stewardship. Given the dynamic environment in which these issues exist, these white papers should be viewed as works in progress. Consequently, we invite interested parties to submit comments, criticisms and suggestions.

To submit comments, please send your emails to dmelamed@melamedia.com

Melamedia, LLC
8315 Riverside Rd.
Alexandria, VA 22308
(703) 704-5665
www.melamedia.com

Executive Summary

HIPAA/HITECH Act Enforcement: 2003-2013
The Role of Patient Complaints in Medical Privacy and Data Security
July 2013

This white paper examines the role patient complaints have played in the enforcement of HIPAA and the HITECH Act in the first 10 years of HIPAA enforcement. Specifically, this white paper examines:

- The number of patient complaints that the HHS Office for Civil Rights (OCR) has received in its first decade of enforcement;
- The complaints that have fallen outside of OCR's jurisdiction as well as within it;
- The effects of breach reporting on the number and quality of patient complaints;
- The role of patient complaints in OCR's resolution agreements; and
- The distinctions between the protection of patient data (security) and the use of patient data (privacy) in the enforcement of HIPAA and the HITECH Act.

Among the major conclusions:

- OCR operates in an environment that is dominated by reports and complaints that are related to data security. Because OCR has the responsibility to enforce patient rights under the Privacy Rule as well, the agency may feel increasing pressure to more aggressively punish covered entities for data use violations through resolution agreements and other measures to reassure the public of its commitment to problems that are outside of data security.
    - In the first 3.5 years of the HITECH breach notification regime, OCR received approximately four times as many reports of violations than it received under the HIPAA complaint program in 10 years.
    - Many patient complaints that were lodged with OCR may have been related to data security. Two of the three leading reasons for complaints are arguably related more to data security rather than to data use. It is unclear to what extent data security-related violations were involved in the leading reason for complaints, "*impermissible uses and disclosures*." This is because "*impermissible uses and disclosures"* could involve either data security violations or data use violations, and OCR has not publicly made these distinctions very clearly.
    - All 12 of resolution agreements OCR imposed in the first 10 years of HIPAA enforcement addressed issues primarily related to data security.
    - In the one instance in which OCR imposed civil monetary penalties, it focused on the patient right to access his or her medical records. However, that case did not involve an entity that regulators or the industry could reasonably view as a rational organization in that it refused to respond to OCR during its investigation.

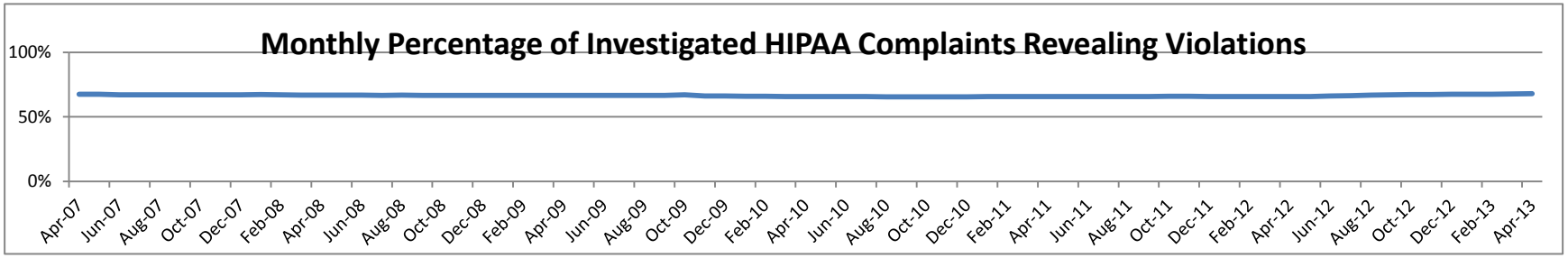
Actionable HIPAA Complaints and HITECH Breach Reports		
April 14, 2003 – April 30, 2013 120 Months	**Sept. 23, 2009 – April 17, 2013 43 Months**	
Investigated Complaints Revealing a Violation	**HITECH Major Breaches Presuming a Violation**	**HITECH Small HITECH Breaches Presuming a Violation**
19,726	**587**	**79,000**
Total: 19,726	**Total: 79,587**	

- Patients have not lodged substantially more complaints because of the HITECH Act breach notification requirements although approximately 23 million patients have been notified of these incidents as of April 17, 2013. Although the overall monthly range of complaints increased from 500-700 to 800-1,000, more than 60% of the complaints OCR received fell outside of its jurisdiction. This area requires further research.

Some possible explanations include:

- Covered entities are not required to inform patients of their right to lodge complaints with OCR in their breach notices.
- Most breaches are minor in nature and are of little concern to patients.
- Patients are satisfied with the explanations given by healthcare organizations.
- Patients feel like there is very little chance of success in obtaining damages from a law suit.
- Patients have become inured to breach notices.

- The percentage of OCR complaint investigations confirming a HIPAA violation has not increased because of the breach notification requirements, but the raw numbers of complaints finding a violation appear to have risen.



- Patients appear to still not understand their rights under HIPAA after the HITECH breach notification requirements went into effect. Prior to the HITECH Act, about 65.8% of complaints were outside of OCR's HIPAA jurisdiction. As of April 30, 2013, it was still 60.7%. This suggests that OCR could play a valuable role in serving as a clearinghouse for complaints regarding health data use and protection that qualify for action under other laws and by other federal agencies.

- The terminology that OCR uses to describe violations under HIPAA and the HITECH Act regulations is confusing and blurs the distinctions between privacy (data use) and data security. This may provide the agency with easier ways to pursue violations, but the terminology can increase the anxiety of the healthcare workforce and thus lead to unnecessary obstacles to the sharing of patient information for treatment and quality purposes.

  For example, it is not obvious to the workforce and the public what the differences are between "*unauthorized access/disclosure"* under the breach rules and "*impermissible uses & disclosures"* under the Privacy Rule and Security Rule. Understanding these distinctions is important because a simple error could be subject to regulatory action under three different rules. This vagueness obscures the distinction between data use and data security and could create obstacles to the sharing of patient information when data protection should be the focus. This is a concern, given the ongoing problems with sharing data due to privacy concerns and the inclusion of thousands of new entities under HIPAA in September 2013.

Methodology

The tables and statistics cited in this white paper are based on enforcement statistics supplied by OCR. Some statistics cited in this white paper are based on reports in *Health Information Privacy/Security Alert*, which obtained enforcement statistics from OCR and CMS in the years before the agencies decided to release them publicly on a regular basis. The analysis did not examine the effect of state breach notification laws.

Introduction

This is the first of a series of white papers examining the first 10 years of enforcement of the HIPAA privacy and security requirements. This white paper focuses on the role of patient complaints and how they have been affected by the HITECH Act breach reporting requirements. The goal is to encourage a practical discussion of how patient data stewardship requirements should be enforced to appropriately balance the need for data sharing for treatment and quality purposes with the need to protect and engage patients.

In the first 10 years of HIPAA enforcement, the healthcare industry has undergone significant changes. The most notable ones were reflected in the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The 2009 law imposed breach reporting requirements on healthcare entities, accelerated the industry's conversion to electronic health records (EHRs) and put thousands of business associates and subcontractors under the jurisdiction of HIPAA. These newly covered organizations are likely to find the security and privacy requirements complicated if the experience of covered entities is any guide.

As important, the HITECH Act re-emphasized the need to instill patients with confidence that the healthcare industry will take adequate steps to ensure the integrity and confidentiality of their medical records. The success of the healthcare system and EHRs relies on patient engagement – a partnership with the healthcare system. So it is crucial to reach an equilibrium that accommodates the flow of patient information for treatment and quality improvement with patient rights over their information.

Under HIPAA, the HHS Office for Civil Rights (OCR) provided patients with the right to lodge complaints. OCR, in turn, decided that it would use its discretion under HIPAA to review and investigate all of these complaints. Implicit in the law and that system was the thought that disciplining the offender for violations created an adequate balance in ensuring the flow of health information while protecting patients.

Acceptance of this approach was reflected in Congress' decision not to give patients the right to sue under HIPAA when it enacted the HITECH Act.

The breach reporting requirements under the HITECH Act, however, required covered entities to disclose their HIPAA violations – not wait until someone complained. OCR again had to decide how to use its discretion in responding to these breach reports. Instead of adopting its approach to patient complaints, OCR decided not to automatically investigate each breach report, but use its discretion in deciding which incidents to pursue.

Given this environment, it is not a surprise that the world of patient data stewardship is one distracted by anxiety over legal and regulatory interpretations and the potential for lawsuits. The purpose of these white papers is to reduce that anxiety and clarify where the real world risks and responsibilities lie.

The HIPAA Enforcement Structure

An understanding of the role patient complaints play in HIPAA enforcement requires an understanding of how they fit into the overall enforcement structure.

The patient data stewardship requirements under HIPAA and the HITECH Act are enforced largely by OCR.[1] The patient privacy and data security complaint system under HIPAA is only one element of OCR's enforcement program.

For the purposes of this white paper, the OCR enforcement structure can be sorted into eight categories.[2]

1. HIPAA Privacy & Security Patient Complaint System
2. HITECH Breach Reporting Requirements for Incidents Involving 500 or More Patients
3. HITECH Breach Reporting Requirements for Incidents Involving Fewer than 500 Patients
4. OCR-Initiated Compliance Reviews
5. OCR Audit Program
6. OCR Resolution Agreements
7. HIPAA Civil Monetary Penalties
8. Criminal Referrals to the U.S. Justice Department[3]

The HIPAA Patient Complaint System

Since April 14, 2003, OCR operated only the Privacy Rule complaint system. That changed in July 2009 when it assumed responsibility for enforcement of the HIPAA Security Rule from the Centers for Medicare and Medicaid Services (CMS). In creating this structure, the Bush Administration decided that it would use its enforcement discretion to respond to every complaint submitted by a patient. That policy continued under the Obama Administration.

---

[1] The Federal Trade Commission has some authority in protecting patient health information under the HITECH Act. It has taken steps on its own and in conjunction with OCR to ensure security of protected health information. From a HIPAA/HITECH perspective, the FTC also has jurisdiction over personal health records when offered by organizations that are not covered by HIPAA. In a broader context, the Federal Trade Commission enforces other laws that provide protection for patient information. Other agencies also have jurisdiction over the confidentiality of patient information. Some of these agencies include Substance Abuse and Mental Health Services Administration, the Equal Opportunity Employment Commission, Occupational Safety and Health Administration, the National Labor Relations Commission and, the Department of Education and many others. For the purposes of this white paper, we are confining this discussion to OCR.

[2] These are not the only elements for enforcing HIPAA and HITECH Act. There are at least three others elements, which will be addressed in future white papers. These three include:

1. Patient law suits in the federal and state court systems
2. The criminal prosecution of individuals who violate HIPAA
3. The ability of state attorneys general to sue covered entities on behalf of their citizens under HIPAA

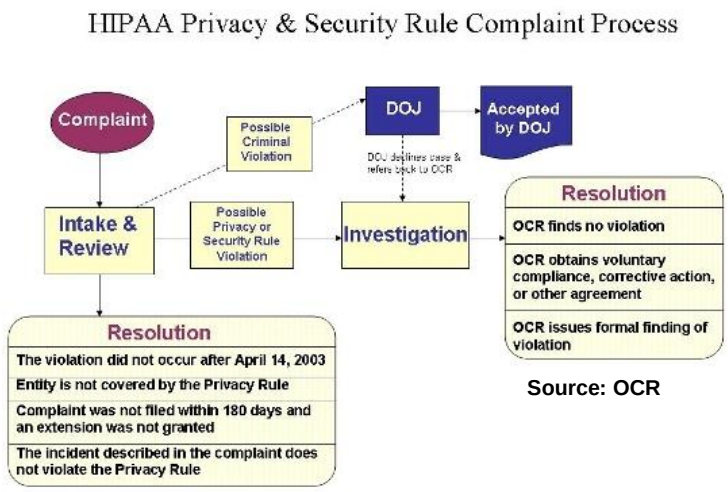
[3] In addition, OCR cooperates with the HHS Inspector General, CMS and other healthcare enforcement authorities to pursue criminal prosecutions involving the defrauding of Medicare and Medicaid.

From the beginning, the systems were related because OCR and CMS occasionally cooperated in cases that substantially involved both regulations. OCR started first, has had the larger budget for HIPAA enforcement, and consequently it has been the agency most associated with this process.[4]

Before OCR took over CMS's responsibilities in 2009, OCR already had jurisdiction over some security-related areas. The Privacy Rule included a "mini-security rule," which required covered entities to take some measures to protect health records. HHS recognized that there could be no confidentiality without some form of data security.

As significant, the Privacy Rule had a wider reach than the Security Rule because the Privacy Rule covers both paper and electronic records. The Security Rule covers only electronic records.[5]

The vast majority of complaints fall under the Privacy Rule. OCR, and CMS before it, attributed the much lower number of Security Rule complaints to the nature of these violations; they typically would be noticed only by workforce members and other insiders.[6] As discussed later, OCR said the breach notification requirements under the HITECH Act have become "one of the primary sources of how we are notified of Security Rule concerns." [7]



Source: OCR

Anyone can file a complaint about a suspected violation of the Privacy Rule or the Security Rule. Upon receiving a complaint, OCR will determine whether it falls within its jurisdiction. Common reasons for a complaint falling outside of OCR's HIPAA jurisdiction are: 1) the violation did not involve an entity covered by HIPAA; 2) the event occurred before the HIPAA regulations went into effect; or 3) the complaint was filed more than 180 days after the individual learned of the incident.

If the complaint falls within its jurisdiction, OCR will gather the information it needs from the target of the complaint and the individual filing the complaint. Sometimes, OCR will visit the covered entity as well and conduct a deeper investigation based on the information it received. It then makes a determination on whether a violation has occurred.

At the conclusion of the investigation, OCR issues a closure letter to the individual and the target of the complaint. This letter describes the allegations in the complaint, the facts of the investigation, the findings of violations (if any), and the agency's decision. The letter includes what corrective action was taken by the covered entity to resolve violations.

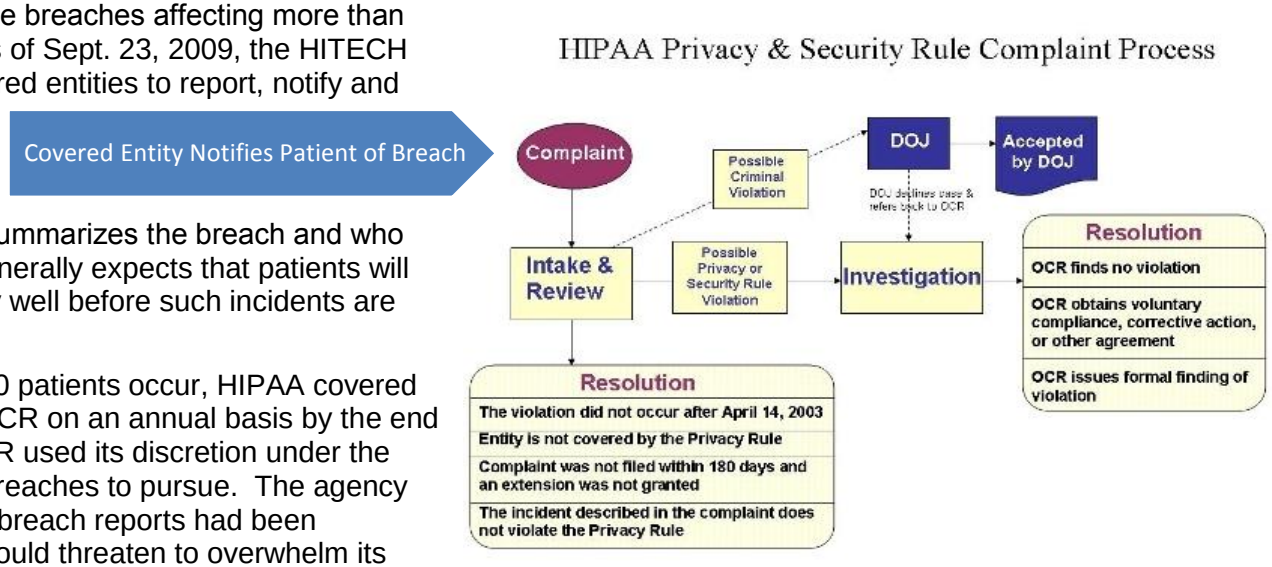
If the individual, who submitted the complaint, disagrees with OCR's conclusion, the agency will respond to the individual and consider additional facts that were not shared during the investigation. The response will vary based on the nature of the concern or the new facts presented.

[4] Because of the delay in adopting the Security Rule, that complaint system went into effect about two years later than the Privacy Rule complaint system on April 20, 2005.
[5] CMS still operates a HIPAA complaint system to investigate suspected violations of the HIPAA electronic transaction standards. However, there have been relatively few complaints, and is beyond the scope of this white paper.
[6] Email Correspondence between Dennis Melamed and Rachel Seeger, Senior Health Information Privacy Outreach Specialist, U.S. Department of Health & Human Services. June 5, 2013.
[7] IBID

The HITECH Breach Notification System

The HITECH Act breach notification requirements complemented the HIPAA privacy and security complaint system in a significant way. When a breach of unencrypted patient data of any size occurs, the covered entity is required to report it to OCR. In addition, the covered entity must notify the affected patients and inform them of what measures have been taken to correct the problem.

The public's attention has focused on the breaches affecting more than 500 patients under the HITECH Act. As of Sept. 23, 2009, the HITECH Act imposed specific deadlines on covered entities to report, notify and mitigate the effects of these larger breaches.



OCR publishes a list of these breaches on a "Site of Shame," which summarizes the breach and who and what was involved. The agency generally expects that patients will have been notified by the covered entity well before such incidents are posted on this site.[8]

When breaches affecting fewer than 500 patients occur, HIPAA covered entities are required to report them to OCR on an annual basis by the end of each February. As noted above, OCR used its discretion under the HITECH Act to decide which reported breaches to pursue. The agency has acknowledged that if these smaller breach reports had been submitted as patient complaints, they would threaten to overwhelm its resources because most – if not all – of the self-reported breaches would be HIPAA violations.[9]

OCR has not been specific in detailing what factors its regional offices should consider in pursuing these reports except that the regional offices should consider the resources they have at their disposal. The assumption is that the same or similar factors that go into pursuing a Privacy Rule or Security Rule investigation also apply to these small breaches.

Nothing prohibits a patient, who receives a breach notice from a covered entity, or anyone else from lodging a HIPAA complaint.

Compliance Reviews and Audits

OCR has the authority to investigate covered entities on its own initiative. It is reasonable to assume that as OCR investigates complaints and receives breach reports (as well as reviewing media accounts and getting other tips from other agencies), that it is using this information to decide when it deems it necessary to conduct such an investigation.

The latest public data on OCR compliance reviews were included in its Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance for Calendar Years 2009 and 2010. It indicated that the agency has conducted dozens of such reviews.

[8] The "Site of Shame" can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

[9] Department of Health and Human Service Fiscal Year 2012, Office for Civil Rights, Justification of Estimates for Appropriations Committees (http://www.hhs.gov/about/budget/fy2012/ocr_cj_fy2012.pdf). Compliance experts note that some entities may be reporting more incidents than necessary to avoid regulatory violations. So some of these reports may not involve breaches although OCR says it presumes they are if the incidents have been submitted. This strategy contrasts sharply with reports that some covered entities are under-reporting incidents.

OCR also started an audit program to help the agency, itself, and the healthcare industry understand the state of HIPAA compliance and identify the biggest problems. The program started as a pilot program examining 115 covered entities representing a cross-section of the industry. The agency announced that it will make this a permanent part its enforcement program after reviewing the results of the pilot program. The agency also said it was reserving the right to punish covered entities for violations discovered during these audits.

When CMS was in charge of enforcing the HIPAA Security Rule, it also engaged in audits in a limited way. The effort was primarily aimed at gaining an understanding of industry practices. Complementing that effort were HIPAA audits by the HHS Office of Inspector General. This too was a limited effort, which did not emphasize enforcement.

Resolution Agreements

The most attention-grabbing tool that OCR uses to encourage compliance is the resolution agreement.

The use of resolution agreements has enabled covered entities to avoid admissions of guilt or penalties – at least in the legal sense. However, they have required covered entities to pay some money for the violations and placed them under federal monitoring programs that subject them to heightened OCR scrutiny and oversight.

According to OCR, the resolution agreements are not based solely on one incident. While a complaint or the news media may publicize an incident, the agency said it typically enters into resolution agreements when the incident reveals a pattern of violations or inadequate compliance systems.

One of the key changes in the HITECH Act was a provision that enabled OCR to keep the money it gets from resolution agreements for enforcement of the Privacy Rule and Security Rule.

Civil Monetary Penalties

The imposition of civil monetary penalties is the harshest action OCR can take on its own. To date, this tool has been reserved for covered entities that have refused to cooperate with OCR in resolving HIPAA violations. The HITECH Act increased the penalties that OCR can impose, and the agency has a four-tiered structure to determine the amount of the penalties. The size of the penalties varies depending on the degree to which a covered entity has taken reasonable steps to establish and maintain an ongoing compliance program.

The HITECH Act also included a provision that requires HHS to develop a methodology to share a percentage of the civil monetary penalties it receives when the patients are harmed by a HIPAA violation. OCR has not yet released its plans for sharing these funds.

OCR Referrals to the U.S. Department of Justice

OCR does not have the authority to pursue criminal prosecutions of individuals or entities that have violated HIPAA or the HITECH Act. Instead, the agency refers them to the U.S. Department of Justice for possible prosecution. OCR recently revealed that the Department of Justice had accepted 54 of the 516 referrals for prosecution in the first 10 years of HIPAA enforcement. [10]

[10] Email Correspondence between Dennis Melamed and Rachel Seeger, Senior Health Information Privacy Outreach Specialist, U.S. Department of Health & Human Services. June 5, 2013.

The Distinctions between Privacy and Security

This white paper draws a distinction between privacy and security in the context of HIPAA enforcement that may be obvious to security professionals, but not so obvious to everyone else. It is an important distinction because it goes to the heart of assessing the legal and regulatory risks that healthcare providers may or may not face when using health information to treat patients. It also helps explain the challenges that face OCR in determining how to approach patient data stewardship enforcement. The blurring of these two concepts obscures OCR's actions for ensuring patient rights over the use of their medical information.

Top Reasons for Patient Complaints
(Source: OCR)

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2010	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Notice
2009	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Complaints to Covered Entity
2008	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Complaints to Covered Entity
2007	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Notice
2006	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Notice
2005	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Mitigation
2004	Impermissible Uses & Disclosures	Safeguards	Patient Access to Records	Minimum Necessary	Authorizations
partial year 2003	Safeguards	Impermissible Uses & Disclosures	Patient Access to Records	Notice	Minimum Necessary

By necessity, the privacy of patient information entails data security. They are not either/or propositions. Nevertheless, they are very different concepts and understanding when they are implicated will dictate the kinds of actions that covered entities must take. Moreover, it determines what regulators and covered entities tell patients about the protection of their medical records.

The use and disclosure of patient information are at the heart of the healthcare industry's mission: providing treatment. Generally speaking, this is what the HIPAA Privacy Rule was designed to regulate. The central questions were: What is the healthcare sector doing with patient information? What limits should be placed on the healthcare sector's use of patient information without patient permission? What rights should patients have in determining what healthcare entities do with their information?

Because the concepts of privacy and data security are closely linked, there is some confusion over the compliance measures required to ensure the appropriate use of patient data under the HIPAA Privacy Rule versus the proper protection of that information.

OCR enforcement actions – particularly the ones capturing the industry's attention – have been primarily aimed at data security-related concerns rather than concerns over the use of patient information as contemplated by the Privacy Rule. Two reasons may be that 1) the Privacy Rule includes a "mini security rule" and covers both paper and electronic records, and 2) the Security Rule covers only electronic health records.

However, these differences may not be readily apparent to the public and do not clearly inform covered entities on the steps they need to take to properly use and protect patient information.

Terminology is important, and it is a challenge under HIPAA and the HITECH Act because one activity can be classified in many different ways. These may be considered very fine or legalistic distinctions. Nevertheless, the failure to understand the differences between *use* and *protection* can result in misdirected or duplicative data management practices or even the failure to appropriately share patient information at all.

A simple example of where this vagueness or overlap occurs is in dealing with employee snooping, which can result in a Privacy Rule violation, a Security Rule violation and a HITECH Act breach report. Physicians and nurses, who are granted access to patient files, but use that access to snoop into other patient records, are violating the Privacy Rule because they are abusing their access rights. They are not using that information to treat a patient. These events would be deemed "*impermissible uses and disclosures"*

of protected health information under OCR's system. The situation gets further muddled as there is a case to be made that this kind of activity would constitute a breach as well and thus could be categorized as "*unauthorized access or disclosure*."

In contrast, when someone, with no permission at all to access patient records, snoops into electronic records, that entity has violated the Security Rule because the entity failed to have adequate access controls, and that triggers the HITECH Act breach notification requirements if the data was not encrypted. Under this scenario, if the records were in paper form, then the Privacy Rule would be triggered instead of the Security Rule, because the Privacy Rule covers paper records.

These two situations clearly require different responses from a covered entity. However, the way OCR reports its enforcement activities does not always make that clear.

OCR created general categories for sorting HIPAA violations in its complaint system. [11] Any analysis is limited because the categories are broad and vague; consequently, it is difficult to pinpoint how violations fall into the category of data security-related concerns rather than into the category of privacy-related data use issues. For example, based on OCR's categories, it can be difficult to understand the differences among a Privacy Rule violation involving *"impermissible uses or disclosures*," a Security Rule violation involving the *lack of "administrative or access controls"* and a HITECH Act breach notice triggered by "*unauthorized access or disclosure*."

Cause of Major Breaches Through April 17, 2013
(Source: OCR)

# of Breaches	Type of Breach	Individuals Affected
300	Theft	8,528,729
101	Unauthorized Access/Disclosure	1,098,402
64	Loss	7,305,104
36	Hacking/IT Incident	1,373,671
24	Improper Disposal	155,133
15	Theft, Unauthorized Access/Disclosure	71,250
11	Theft, Loss	118,979
11	Unauthorized Access/Disclosure, Hacking/IT Incident	459,438
9	Unknown	2,229,805
5	Other	358,617
3	Theft, Unauthorized, Access/Disclosure	4,814
2	Unauthorized Access/Disclosure, Other	65,600
2	Theft, Unauthorized Access/Disclosure, Hacking/IT Incident	14,000
2	Loss, Improper Disposal	3430

When CMS was operating the Security Rule complaint system, it categorized violations in different ways than OCR for the obvious reason that they were responsible for different regulations. When OCR assumed responsibility from CMS, it did not use CMS's terminology in categorizing patient complaints about security or in its public breach reporting statistics. For example, CMS reported that the leading reasons for HIPAA security complaints through August 2008 involved Information Access Management (149), Access Controls (134), Security Awareness and Training (121), Security Incident Procedures (70) and Device and Media Control (61).[12]

In addition to not providing much detail regarding data security in its complaint system statistics, OCR has not provided much detail to link the reasons for patient complaints to the reasons for the data breaches.

The overlapping categories of violations under different rules have the potential to create obstacles to the legitimate sharing of health data because they can be confusing and daunting. An example illustrates the problem. OCR has stated that when a provider (who could be a doctor, a nurse, a pharmacist or some other healthcare professional) mistakenly accesses the wrong patient file in

[11] OCR's rankings are based on cumulative numbers since the beginning of the complaint program. The agency has not released statistics on the nature of the complaints on a monthly basis.
[12] CMS Eases Encryption Requirements on Desk Top Computers (September 2008) Health information Privacy/Security Alert. p.5. Note: In March 2004, Health Information Privacy Alert changed its name to Health Information Privacy/Security Alert.

providing treatment, it does not consider that a violation of either HIPAA or the HITECH Act. It is deemed to be an inadvertent disclosure. Under other circumstances, however, such an activity could be seen as violations of the Privacy Rule, the Security Rule and the HITECH Act.

In other words, the fear of innocent mistakes may inhibit the sharing of information. While the overlapping regulatory authority may make it easier for OCR to enforce patient data stewardship rules, it is easy to understand why some healthcare organizations may adopt overly restrictive data sharing policies when one error could trigger multiple violations under different rules.

Consequently, it is important to make healthcare providers understand that using patient information for treatment purposes is encouraged under HIPAA and the HITECH Act. From a strictly treatment perspective, it is only when healthcare providers fail to protect that information that regulatory problems arise. That is a data security problem, not a data use problem.

Making these types of distinctions as clear as possible may be even more important now because a new universe of entities will be covered by HIPAA as the HITECH Act significantly expanded the law's jurisdiction to include business associates and subcontractors. To be sure, business associates and subcontractors will not be treatment providers with treatment relationships with the patients. However, many of these newly covered entities will be providing services in support of treatment as well as providing services under the payment and healthcare operations provisions of HIPAA, which are exempted from patient permission requirements under the Privacy Rule.

With those points noted, there still are discernible trends. Regardless of how the issues are parsed, data security concerns play a significant – if not dominant -- role in the patient complaint system.

The lack of safeguards, which clearly implicates data security, has been consistently cited as the second leading HIPAA violation reported in patient complaints over the years.

The leading reason for HIPAA patient complaints falls under the category of "*impermissible uses and disclosures*." As noted earlier, this category of activity could be related to either the Privacy Rule or the Security Rule because the complaint could involve the inappropriate use of protected health information for marketing purposes or could be snooping.

It is easy to see why healthcare providers can get confused over the distinctions between the use and protection of patient data because OCR breach statistics indicate that "*unauthorized access/disclosure*" is the second most common reason for a breach affecting more than 500 patients. At the same time, this could constitute an *"impermissible use or disclosure"* under the Privacy Rule. So the healthcare industry is left trying to figure out the difference between an "*impermissible disclosure"* and an "*unauthorized disclosure*."

Location of Major Breaches Through April 17, 2013
(Source: OCR)

# of Breaches	Location	Individuals Affected
135	Laptop	2,329,238
132	Paper	727,731
74	Desktop	2,419,525
73	Other Portable Electronic Device	757,945
58	Network Server	2,427,183
41	Other	2,746,226
9	Email	239,700
7	Electronic Medical Record	120,752
6	Laptop, Desktop	5,303
5	Desktop, Network Server	21,605
5	X-ray film	6,681
4	Backup Tapes	5,969,483
3	Desktop, Electronic Medical Record	19,888
3	Desktop, Paper	3,463
2	Laptop, Paper	6,571
2	CDs	7,172
2	Laptop, Network Server	5,550
2	Other Portable Electronic Device, Electronic Medical Record	17,360
2	Desktop, Other Portable Electronic Device	1,356
2	Network Server, Email	51,848

The location of the data breached more clearly implicates data security violations in OCR's enforcement approach. Theft of paper records would fall under the Privacy Rule, and not the Security Rule. Simply citing a Privacy Rule violation does not mean a HIPAA covered entity violated some restriction on the use of protected health information. Paper records were involved in 139 of all major breaches and were thus covered by the Privacy Rule. But the loss and theft of paper records are data security problems.

The most notable exception to the overt emphasis on data security has been patient complaints over their ability to access their medical records. The failure to provide patients with their records has been consistently the third leading cause of patient complaints.[13]

The leading reason for patient complaints, however, deals with *impermissible uses and disclosures* of patient information. These complaints may reveal many data use violations under the Privacy Rule, but OCR's lack of specificity and the confusing regulatory terminology do not indicate that clearly.

OCR may already be aware of this perception. On June 13, 2013, the agency announced a $275,000 resolution agreement with Shasta Regional Medical Center because senior executives shared patient information with the media without patient permission. Even in this case, however, the agency's focus on security was in evidence as its headline referred to the agreement as resolving Security Rule case and not a Privacy Rule case.[14]

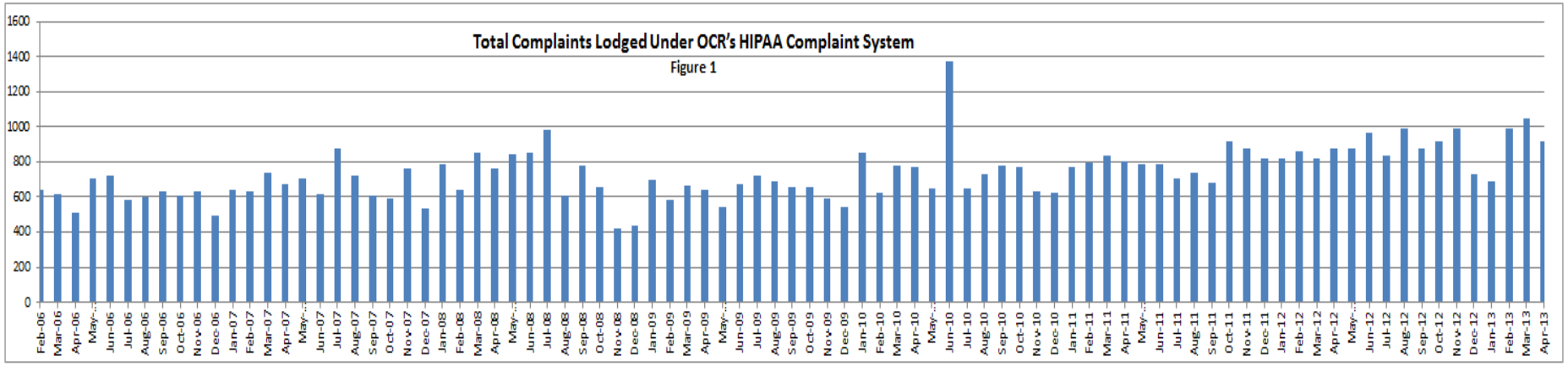
The question is not whether OCR is too focused on data security. There are very good reasons to worry about data security. Instead, the question is what steps OCR will take to show that it is meeting its obligations to enforce violations of the data use provisions of HIPAA – the original reason HIPAA was hailed as creating the nation's first set of patient rights. Because of the blurring of data security and data use issues, the challenge OCR faces is reassuring patients that their health information is being used appropriately while not adding further anxiety and confusion among healthcare providers when sharing information for treatment and quality improvement.

[13] In the wake of the recent Supreme Court decisions on same-sex marriage, problems with access to patient records may gain more attention. These decisions are likely to affect the definitions of a "personal representative" under HIPAA as well as policies granting family members access to patients or their records.

[14] Shasta Regional Medical Center Settles HIPAA Security Case for $275,000, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/shasta-agreement.html, accessed July 11, 2013

HIPAA Patient Complaints & HITECH Act Breaches

From April 14, 2003 through April 30, 2013, OCR received 80,836 complaints through its patient complaint system. Approximately 28,981 were eligible for OCR investigation under HIPAA. Of those, 19,726 revealed a HIPAA violation and required covered entities to change their policies and/or procedures; another 9,255 investigations found no violation.



Approximately, 44,695 complaints were outside of OCR's jurisdiction because the actions occurred before the regulations went into effect or they were filed more than 180 days after discovery of the incident or were outside HIPAA's jurisdiction. Approximately 7,160 complaints were in some stage of review or investigation.

In contrast, from Sept. 23, 2009 when the HITECH Act breach reporting requirements went into effect, through April 17, 2013, OCR received reports of 587 major beaches, which affected about 22 million patients. The agency also received approximately 79,000 reports from covered entities on smaller breaches, which affected fewer than 500 patients. Taken together, these smaller breaches affected hundreds of thousands of patients.[15] [16]

These smaller breaches would have required OCR action if the incidents had been submitted as patient complaints under the agency's current policy.[17] OCR has acknowledged that it does not have the resources to investigate all of the smaller breach reports. In its budget request of fiscal year 2012, the agency acknowledged that almost all breach reports affecting fewer than 500 individuals were not being investigated. [18]

[15] 79,000 Small Breaches, But Some Good News for CEs (April 2013) Health information Privacy/Security Alert. p.1.
[16] OCR stated in a July 1, 2013 email to the author that as of July 1, 2013, OCR has received more than 81,000 small breach reports affecting more than 915,000 patients. Email Correspondence between Dennis Melamed and Rachel Seeger, Senior Health Information Privacy Outreach Specialist, U.S. Department of Health & Human Services. July 1, 2013.
[17] These self-reported smaller breaches may reflect a conservative estimate as regulators suggest that there is continued under-reporting of breaches.
[18] OCR Budget Increases, Calls for More Enforcement, (February 2011) Health information Privacy/Security Alert. p.1. It should be noted that while OCR has suggested that many of the smaller breach reports have been minor or one-off leaks, such as a misaddressed bill, many of the privacy complaints only affect a very limited number of people as well.

To summarize the situation: the OCR statistics indicate that in about one third of the period of time, the breach reporting requirements identified more than four times the number of HIPAA violations involving the security of patient information than the HIPAA complaint system investigations finding data use violations: 19,726 patient complaint investigations revealing privacy and data security violations versus 79,587 breach reports revealing data security violations.

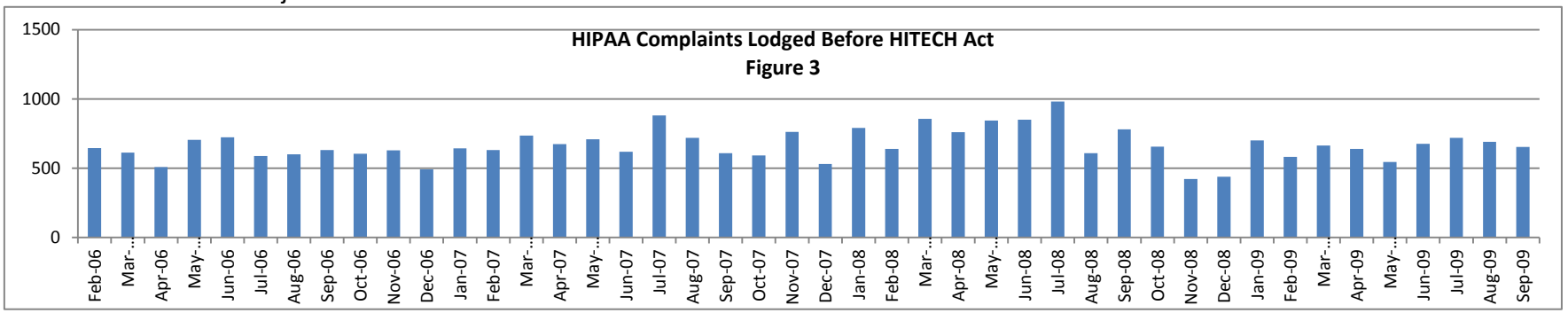
HIPAA Complaints Revealing a Violation and HITECH Breach Reports Figure 2		
April 14, 2003 – April 30, 2013 120 Months	Sept. 23, 2009 – April 17, 2013 43 Months	
Investigated Complaints Revealing a Violation	HITECH Major Breaches Presuming a Violation	HITECH Small HITECH Breaches Presuming a Violation
19,726	587	79,000
Total: 19,726	Total: 79,587	

Some breach reports have resulted in patient complaints, which in turn, have resulted in OCR investigations. OCR has not published statistics on this interaction. However, the discussion below reveals that generally, the HITECH Act breach reporting requirements may have increased HIPAA patient complaints, but not dramatically.

One take-away from these statistics is that OCR faces an enforcement environment that has been dominated by data security issues and not patient privacy (data use) or other patient rights issues under HIPAA.

Is the Breach Reporting System Resulting in More Patient Complaints?

At first blush, it would seem that as patients were notified of breaches, many would be motivated to file a complaint with OCR. Again, more than 22 million patients have been notified that their medical information had been breached because of a major incident and hundreds of thousands have been notified because of smaller incidents.



Since the beginning of the HIPAA complaint system, the number of patient complaints has increased gradually. Figure 3 shows the number of complaints filed with OCR prior to the HITECH Act.[19] Overall, the number of complaints from February 2006 through August 2009 was in the range of 500 to 700 per month.

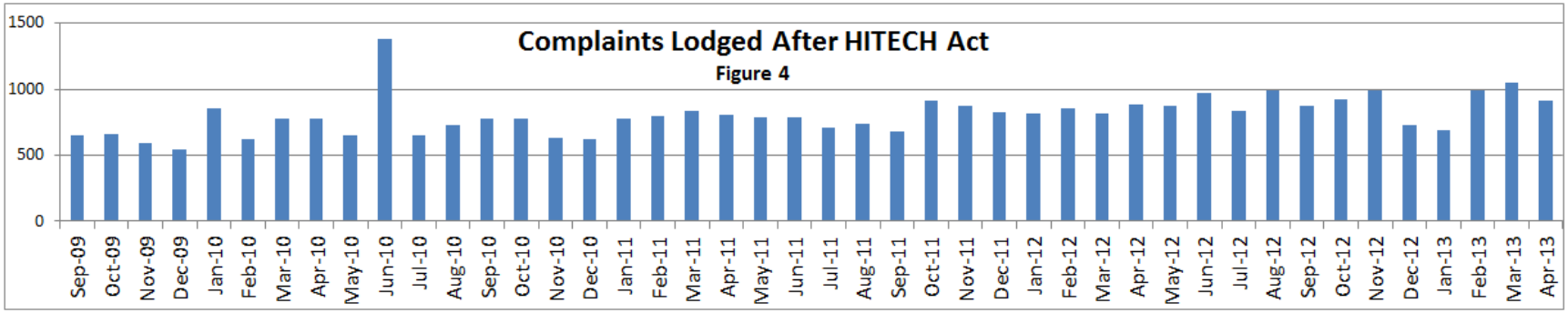
[19] While the complaint system was established in April 2003, statistics were not available until February 2006. Earlier numbers also would not be representative of overall patient activity as the program was new and presumably largely unknown to the public.

There are some notable spikes, such as in July 2007 and July 2008. The reasons for these spikes are not clear. Some possible explanations include publicity about a large breach or a series of breaches; attempts by class action attorneys seeking to create classes of patients to sue over HIPAA violations or some other reason.[20] More research is needed to understand the reasons for the fluctuations in the number of monthly complaints.

The July 2007 spike quickly disappeared and complaints diminished, but slowly started to rise again from February 2008 and culminated with 1,000 complaints in July 2008. Then, the level of complaints declined sharply again through November 2008 to the lowest level since before February 2006. The number of complaints again grew slowly through August 2009.

One common explanation for the decline in complaints starting in August 2008 was the recession under the theory that people sought fewer healthcare services to save money and thus had fewer encounters with covered entities. Again, the reasons for these spikes are unclear, and more research is needed to understand this dynamic.

Figure 4 reflects complaints that were lodged after the HITECH Act breach notification requirements went into effect on Sept. 23, 2009. The chart indicates the levels of complaints rose and were in the range of 800 and 1,000 per month. While it is tempting to suggest that breach reporting increased the number of complaints, there is little evidence to prove that it accounted for all the growth, although it is likely that it played a role. One reason for this



circumspection in attributing the increase to the HITECH Act was the absence of a sustained increase in complaints once breach reporting started.

In fact, the rate declined through the remainder of 2009 despite media coverage of the major breaches and the creation of OCR's Site of Shame on which covered entities and their business associates were listed and the breaches summarized.

It is important to note that OCR generally expects that patients have been notified already of a breach before the incident is posted on the agency's Site of Shame. Furthermore, nothing requires a patient to immediately file a HIPAA complaint upon learning of a breach although it does trigger the 180-day deadline for making such complaints. However, one would expect that patients would be the most motivated to file a complaint after learning of a breach

[20] Another possible reason could be media reports of states adopting their own breach notification reporting laws. It also is conceivable that the increases represented protests of some kind because anyone can file a complaint with HIPAA. While there is nothing to suggest that this has happened, it is a possibility given the effect that a small number of complaints could have on the overall statistics. Again, this area requires further study, and the reasons remain speculative.

and that as time passes, the interest in filing a complaint would diminish. At the same time, patients may still not be aware of their right to lodge a complaint under HIPAA. Covered entities are not required to inform patients of this right when they are notified of breaches.

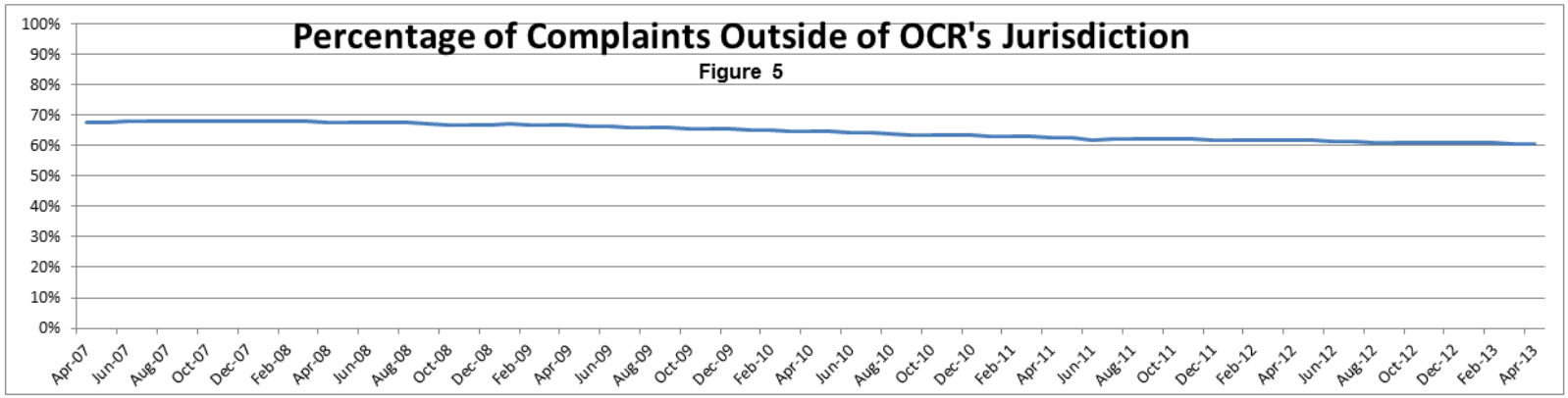
There was a significant spike in complaints in June 2010, but then the level of complaints fell quickly although the overall trend in the number of complaints continued to be in the range of 800 to 1,000 complaints.

Whether the increase in patient HIPAA complaints resulting – at least in part -- from these breach notices is meaningful depends on one's vantage point. From a percentage perspective, the growth may seem significant although small shifts in the raw numbers can result in significant changes. From another perspective, the increase may seem disappointing given the number of patients who were notified of breaches. And from yet another vantage point, the overall number of complaints may seem heartening given the huge number of patient interactions and vast data sharing that occur in the healthcare sector.

The reason for the increase in patient complaints is an area that merits further study. In the meantime, the magnitude of the increase could be explained by the fact that covered entities were required to inform patients of what steps were taken to rectify breaches, thus reducing the motivation to file a complaint. If true, this could provide support for OCR's enforcement posture of punishing the offender rather than compensating the victim. On the other hand, it could reflect either weariness with receiving breach notices generally or that the ability to sue and win damages in court is limited.

Is OCR Receiving More Complaints that Fall Under OCR's Jurisdiction? [21]

As the public becomes more aware of healthcare's data stewardship responsibilities through breach notifications, it would be reasonable to assume that patients would be lodging more complaints that would require OCR action. However, the data is not definitive.



When the breach reporting requirements went into effect on Sept. 23, 2009, the percentage of complaints that fell outside of OCR's jurisdiction was approximately 65.8%. As of April 2013, that percentage gradually fell to approximately 60.7%. (See Figure 5)

[21] The data in the remainder of these charts start from April 2007 when OCR started providing more detailed information on the complaint program.

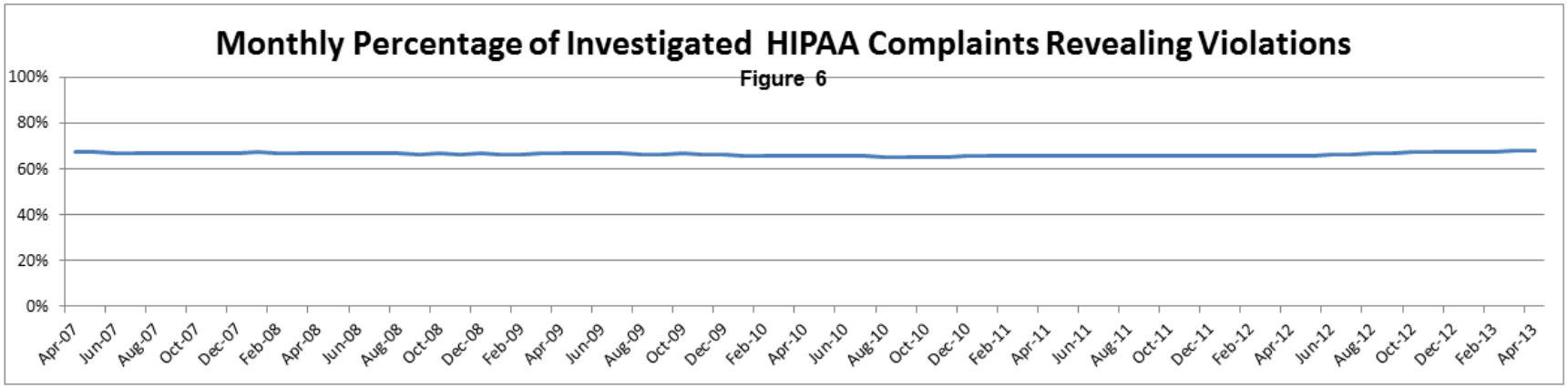
Whether the decline is attributable to the HITECH Act is unclear, although again it is likely to have been a contributing factor. It could also reflect who was filing complaints. Healthcare employees may be more apt to file complaints then the general patient population. OCR (and CMS before it) has often acknowledged that this was the case in regard to Security Rule complaints. Also there are some indications that those healthcare employees, who challenge their terminations, increasingly are alleging that their employers have been violating HIPAA.[22]

There also is no data to determine how many of these pre-HITECH complaints targeted business associates or subcontractors and thus were outside of OCR's jurisdiction before Sept. 23, 2009. So it remains to be seen whether the expansion of HIPAA to cover contractors and subcontractors will increase the number of actionable patient complaints.

These contractors and subcontractors are often unknown to the patient so the breach reporting requirements are likely to remain the leading sources of HIPAA allegations, particularly those involving Security Rule problems. That is because the HITECH Act has expanded the population of covered entities, and more HIPAA complaints from workforce members may be forthcoming.

Complaints That Revealed a Violation

The level of patient complaints that resulted in findings of a HIPAA violation suggests a modest effect of the breach notification requirements. The rise in the percentage of confirmed violations was minimal. In April 2007, the percentage of actionable complaints that revealed a violation was approximately 67.5%. By April 2013, the rate was



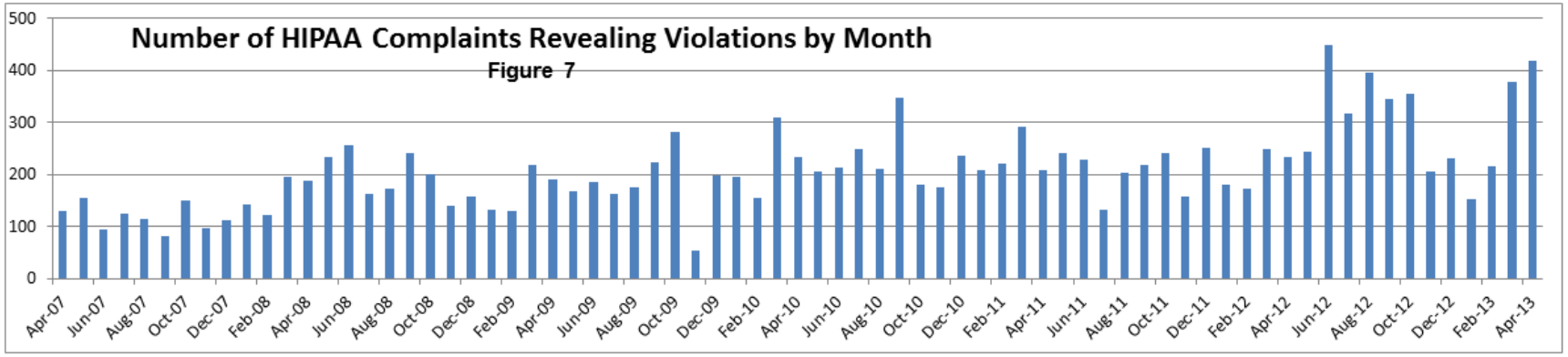
68%. However, the percentage of complaints revealing a violation actually declined slightly for more than a year after the HITECH Act requirements went into effect.

To be fair, it is important to remember that despite the criticism aimed at the healthcare industry, many covered entities have taken substantial actions to comply with HIPAA. Consequently, the responsible behavior of these organizations would be expected to have a dampening effect on the level of reported violations.

[22] A separate white paper examining the role of patient complaints and OCR investigations will address these issues.

As noted earlier, the breach notification reports are most likely to reveal Security Rule infractions. For example, these breaches suggest that many covered entities may have made a mistake in deciding to not encrypt their data yet there was not a substantial increase in Security Rule complaints.[23]

Since OCR took over enforcement of the Security Rule in 2009, it has received approximately 709 complaints.[24] The number of Security Rule complaints is less than 1% of the breach reports that OCR has received during about the same period of time.

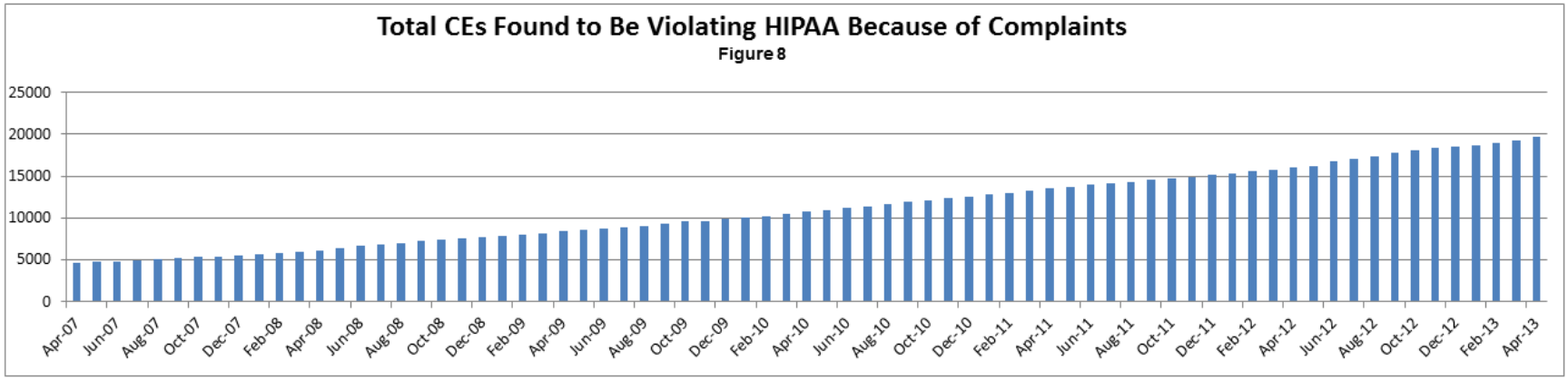


Over the course of the HIPAA program, the number of complaints that revealed violations on a monthly basis has grown gradually but in a highly variable manner. In terms of the raw number of cases, Figure 7 reveals a discernible overall increase in the number of complaints that uncovered HIPAA violations. This could be explained by the overall increase in actionable complaints. It also could be attributed to OCR's experience with enforcing the regulations.

In assessing this aspect of enforcement, it is important to recognize that the resolution of these complaints typically occurs months after they have been lodged. As a result, if there were large breaches or other events that provoked complaints, they may not appear in OCR's statistics until months later and not necessarily as a group.

[23] The Security Rule does not require covered entities to encrypt patient information. It is considered an "addressable implementation standard" under HIPAA. In other words, a covered entity can decide for itself when it would be appropriate to encrypt the data. However, it does have to document its justification for its decision. Under the HITECH Act, if data has been appropriately encrypted, a breach has not occurred regardless of whether it has been lost, stolen or hacked.

[24] HIPAA and Breach Enforcement Statistics for June 2013, published by Melamedia, LLC, accessed June 1, 2013. http://www.melamedia.com/HIPAA.Stats.0613.html



The raw number of complaint investigations as illustrated in Figure 8 are cumulative – and not on a month-to-month basis – but still show confirmed HIPAA violations rising more quickly starting in the spring of 2010. On the other hand, OCR announced that it would be more aggressive after more than five years of focusing on educating the industry.

Complaints, Breaches & Resolution Agreements

The resolution agreement is OCR's most publicized enforcement tool. In these instances, OCR has deemed that the violations uncovered by its investigations require a more significant response than requiring relatively minor or low-key changes by the covered entities. There have been 12 resolution agreements during the first 10 years of HIPAA enforcement. All of them were reached more than five years after the Privacy Rule went into effect.

The small number makes it difficult to draw general conclusions except to indicate where OCR has decided to send a message to the industry at a particular point in time. That message emphasized data security.

Five of these resolution agreements originated with patient complaints. The underlying theme of most of the12 resolution agreements was the failure to have proper security controls in place.[25] Two cases were cited as involving Privacy Rule violations, but could be deemed to be security-related and not data use-related. In these two incidents, Rite Aid and CVS were cited for improper disposal of non-electronic protected health information

OCR Resolution Agreements April 2003 – April 2013			
Covered Entity	**Date**	**$ Amount**	**Patient Complaint**
Idaho State University	May 12, 2013	400,000	
Hospice of North Idaho	Dec. 31, 2012	50,000	
Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc.	Sept. 17, 2012	1,500.000	
Alaska DHSS	June 26, 2012	1,700,000	
Phoenix Cardiac Surgery	April 13, 2012	100,000	Yes
BCBST	March 13, 2012	1,500.000	
UCLA Health System	July 6, 2011	865,500	Yes
General Hospital Corp. & Massachusetts General Physicians Organization, Inc.	Feb. 14, 2011	1,000,000	Yes
Civil Monetary Penalty Cignet Health of Prince George's County, MD	Feb. 4, 2011	4,300,000	Yes
Management Services Organization Washington, Inc	Dec. 13, 2010	35,000	Referral from OIG
Rite Aid Corporation	July 27, 2010	1,000,000	
CVS Pharmacy, Inc	Jan. 16, 2009	2,250,000	
Providence Health & Services	July 16, 2008	100,000	Yes

[25] The resolution agreement with Management Services Organization Washington, Inc. was part of a larger case that referred by the HHS Office for Inspector General and involved violations of the False Claims Act.

(paper documents and pill bottles with labels). As noted elsewhere, the reason these violations were not considered Security Rule violations was because only the Privacy Rule covers paper records.

Five of the last six resolution agreements reviewed resulted from HITECH Act breach reporting; only one resulted from a patient complaint.

Civil Monetary Penalties

The only instance to date that involved a civil monetary penalty was the subject of patient complaints. It is the only one that did not involve a privacy or data security right. It addressed a patient's right to access his or her medical records. However, this case has been considered an outlier for compliance and liability purposes because the entity did not challenge the appropriateness or legality of HIPAA. It simply refused to respond to OCR when it conducted its investigation. Such irrational behavior by an organization is outside the scope of this analysis.

It is important to note, though, that the HITECH Act included a provision that requires HHS to develop a methodology to share a percentage of the civil monetary penalties it collects with the patients harmed by a HIPAA violation. Moreover, the existence of these penalties is expected to provide a deterrent against entities that ignore their patient data stewardship responsibilities.[26]

There is a sense among some experts that the penalties, even before they were increased by the HITECH Act, were more "useful" in marketing legal and compliance services and products rather in encouraging HIPAA compliance itself. Consultants, attorneys and publishers warned of stiff penalties for HIPAA violations even as OCR was reassuring the industry during the first five years of enforcement that it wanted to encourage compliance, not punish healthcare organizations.[27]

[26] As this white paper was being developed, OCR announced a resolution agreement involving the inappropriate sharing of information with the media. However, this occurred in July 2013. This white paper only addresses HIPAA enforcement through April 2013.

[27] To be fair, there is a strong case to be made that the mere existence of the penalties had the intended effect of prompting compliance. If the law contained no penalties, there would be absolutely no incentive to comply with the law. The lack of penalties would have reduced HIPAA to a "voluntary" compliance program and not a mandate to change practices. Nevertheless, and perhaps unavoidable, the threat of penalties did provide a way for marketers to scare covered entities by overstating the real threat of enforcement. For example, a few months after the Privacy Rule went into effect, the author received an advertisement for a "HIPAA-compliant" fax machine that cost thousands of dollars. There is and was no such thing as a HIPAA-compliant fax machine. In fact, there is nothing that is HIPAA compliant. Products and services may be capable of meeting HIPAA requirements, but compliance relies on how covered entities deploy and use those products and services to manage and protect patient data.

Invitation to Comment

This white paper and those to follow are intended to foster an ongoing discussion of patient data stewardship. Given the dynamic environment in which these issues exist, these white papers should be viewed as works in progress. Consequently, we invite interested parties to submit comments, criticisms and suggestions.

To submit comments, please send your emails to dmelamed@melamedia.com

Melamedia, LLC
8315 Riverside Rd.
Alexandria, VA 22308
(703) 704-5665
www.melamedia.com