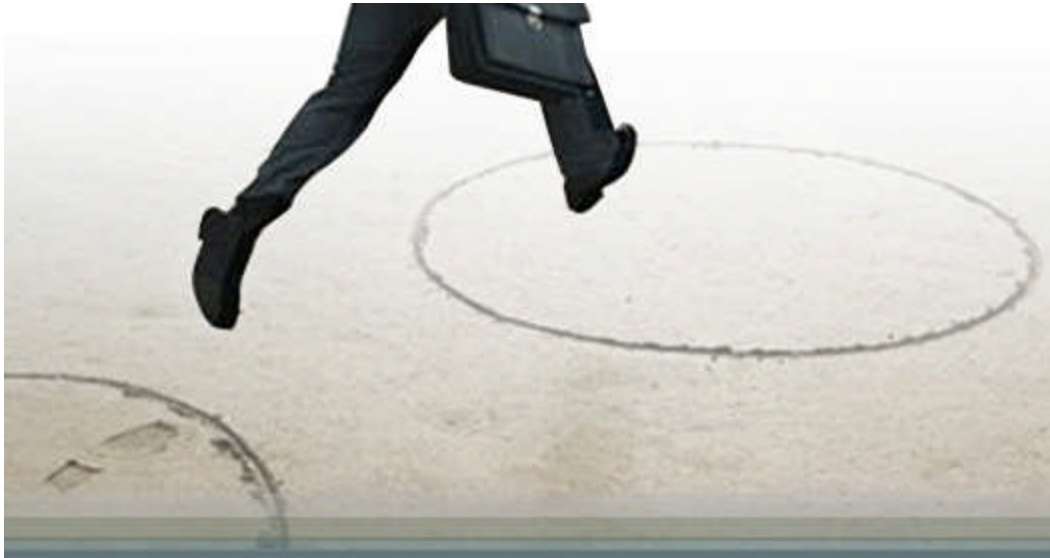
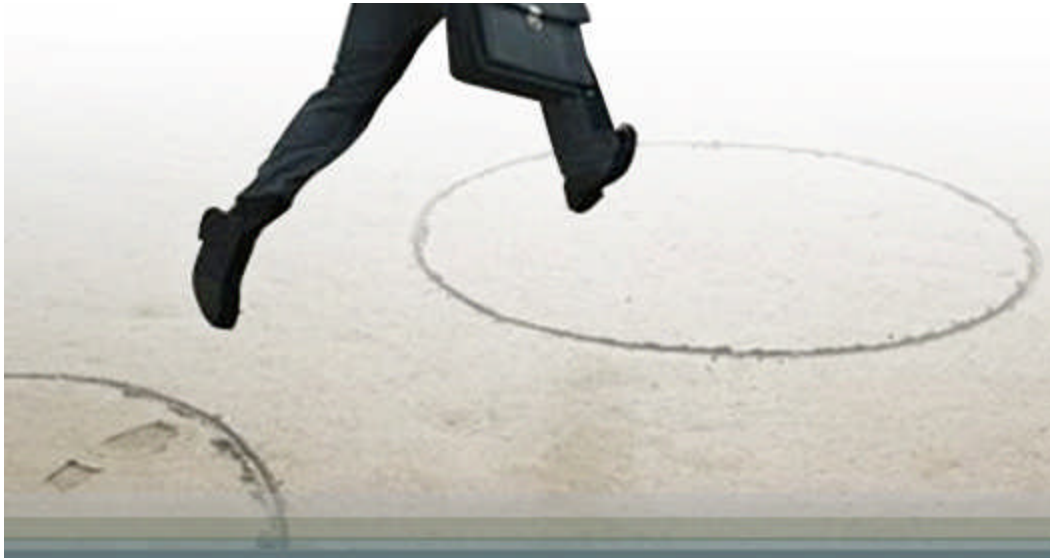


crowell moring

Recent Enforcement Actions under HIPAA and What They Mean for Covered Entities and Business Associates

The webinar will begin shortly. The slides and a recording of the webinar will be sent to you.



crowell moring

Recent Enforcement Actions under HIPAA and What They Mean for Covered Entities and Business Associates

Christine Rinn
Barbara Ryland

April 12, 2011

Introduction

- Settlements and the imposition of civil monetary penalties ("CMPs") by the Department of Health & Human Services ("HHS") Office for Civil Rights ("OCR") highlight the need post-HITECH for covered entities and business associates to implement comprehensive and effective HIPAA privacy and security programs as well as the ramifications of failing to cooperate with OCR investigations into alleged violations.

The Enforcement Actions

- February 22, 2011 - OCR issued a Notice of Final Determination finding that Cignet Health of Prince George's County, MD violated the Privacy Rule. HHS imposed a CMP of $4.3 million for the violations, representing the first CMP issued by the Department for violations of the HIPAA Privacy Rule.

The Enforcement Actions

- February 14, 2011 - Resolution Agreement with The General Hospital Corporation and Massachusetts General Physicians Organization, Inc. to settle potential violations of the HIPAA Privacy and Security Rules. Mass General agreed to pay $1,000,000 and enter into a Corrective Action Plan ("CAP") to implement policies and procedures to safeguard the privacy of its patients.

The Enforcement Actions

- December 13, 2010 – OCR entered into a Resolution Agreement with Management Services Organization Washington, Inc. ("MSO"), to settle potential HIPAA violations. Settlement arose from and was made in coordination with the HHS OIG and Department of Justice, which had been investigating MSO for violations of the Federal False Claims Act.
- MSO agreed to pay $35,000 and implement a detailed CAP.

Civil Enforcement – Basics

- Civil enforcement statute is found at 42 U.S.C. 1320d-5. It was amended by Section 13410(d) of the HITECH Act, effective February 18, 2009.
- Enforcement regulatory provisions are found in 45 C.F.R. 160.401 *et seq.*
- The Secretary issued interim final regulations on October 30, 2009 implementing the HITECH enforcement provisions.

Civil Enforcement – Basics

- OCR performs audits, investigations of complaints and imposes civil penalties. Prior to HITECH, OCR mostly worked with covered entities to obtain voluntary compliance.
- First significant penalty was not imposed until 2009 nearly six years after Privacy Rule and four years after Security Rule became effective.

Civil Enforcement – HITECH

- HITECH did not significantly change the substantive Privacy and Security Rule standards – but the HITECH Act significantly strengthened civil enforcement provisions.
- Expanded the Secretary's authority in key areas:
  - Business Associates
  - Civil penalties for criminal violations
- Established statutory levels of culpability and set forth legislative expectation for the imposition of penalties, with leniency being the exception rather than the rule.
- Expanded enforcement through State AGs.

Civil Enforcement – HITECH

- HITECH Act requires the Secretary to formally investigate any complaint of a violation if a preliminary investigation of the facts of the complaint indicates that a possible violation is due to willful neglect.
- As of February 18, 2011, Secretary also has authority to utilize civil enforcement even if the action might have violated the criminal provisions of 42 U.S.C. § 1320d–6(a), so long as no criminal penalty has been imposed for the same conduct. Prior law actually prevented the Secretary from imposing penalties in the most egregious cases – where criminal violations might have occurred

Civil Enforcement – HITECH

- HITECH Act requires the Secretary to impose civil penalties if a violation is due to willful neglect.
- HITECH Act favors the imposition of penalties for all but the lowest level of violations:
  - "Nothing in this section shall be construed as preventing the Office for Civil Rights of the Department of Health and Human Services from continuing, in its discretion, to use corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) of the violation involved."
- i.e., the Secretary should forego imposing penalties only for the lowest level of infraction.

Business Associates

- 42 U.S.C. § 17931 makes key security standards applicable to business associates, in the same manner that such sections apply to the covered entity.
- HITECH security standards are also applicable to business associates.
- Business associates are subject to civil and criminal penalties for violation of any security provision, and can incur penalties for violating the terms of business associate agreements.

Business Associates

- Covered Entity has liability for BA's actions only if
  - CE failed to require the BA to adhere to required standards or
  - CE knew of a pattern of violations and failed to terminate the contract or report the violation.
- Secretary is authorized to conduct audits of both CEs and BAs.

State Attorney General Enforcement

- HITECH Act gave state attorney generals authority to enforce HIPAA provisions on behalf of state residents and to obtain injunctive relief and damages, as well as attorney fees
  - Requires notice to the Secretary and allows the Secretary to intervene.
  - The state may not bring an action under this provision if a federal action is pending.
  - Penalty structure for AG enforcement is different, and maximum penalties are lower.
  - Main use will likely be for injunctive relief to stop or avoid violations, as well as an adjunct to existing state laws that also provide relief or penalties arising out of the unauthorized disclosure or breach of data protections.

Penalty Drivers

- What HIPAA standard was violated?
- What culpability level applies to the violation?
- How many violations occurred?
- Are there aggravating or mitigating circumstances?
- Are there affirmative defenses?
- How do the breach notification provisions relate to the imposition of penalties for HIPAA violations?

What Is a HIPAA Violation?

- A HIPAA violation is linked to the violation of a specific ***provision*** of law, whether statutory or regulatory.
- A "unique" or "single" violation is determined by reference to the statutory or regulatory requirement that is alleged to have been violated (rather than, for instance, the number of unique persons whose PHI was involved).
  - Definitions relevant to what is the basis of a violation are found in 45 C.F.R. § 160.302.
  - Violation or violate means, as the context may require, failure to comply with an administrative simplification provision, which is any requirement or prohibition established by: (1) 42 U.S.C. 1320d--1320d-4, 1320d-7, and 1320d-8; (2) Section 264 of Pub. L. 104-191; or (3) This subchapter (i.e., the Privacy and Security Rules).

What Is a HIPAA Violation?

- Security and Privacy Rules limit the extent to which entities can be assessed separate penalties for "overlapping" provisions.
- Section 160.404(b)(2) limits the Secretary from "double counting" or increasing the number of infractions if a requirement or prohibition is repeated in a more general form in the same subpart. In that case, a civil money penalty may be imposed for a violation of only one provision.
- However, this limitation does not prevent the assessment of multiple penalties if conduct violates distinct provisions of the Security and Privacy Rules; for example, failure to adopt administrative safeguards could violate both the Privacy Rule (§ 164.530(c)) and the Security Rule (§ 164.308). Because these rules are different "subparts," penalties can be independently assessed for violations of both.

What Is the Level of Culpability?

- There are four levels of civil culpability, and penalties are tiered to the level of culpability.
- (1) **Reasonable Diligence:**
  - The person reasonably did not know and, by exercising reasonable diligence, would not have known that the covered entity violated such provision.
  - **Reasonable diligence** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

What Is the Level of Culpability?

- (2) **Reasonable Cause**
- The violation was due to reasonable cause and not to willful neglect
- **Reasonable cause** means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.

What Is the Level of Culpability?

- (3) and (4): **Willful Neglect**
- Violations due to willful neglect are grouped into two categories:
  - (3) Those in which the violation is corrected (within 30 days), and
  - (4) Those in which it has not been corrected.
- **Willful neglect** means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

What Is the Level of Culpability?

- For example: placing records containing PHI in an open dumpster without shredding materials first would almost certainly qualify as a violation that is due to willful neglect.

What Is the Level of Culpability?

» Penalties increase as the seriousness of the infraction increases, and are based on the nature and extent of the violation and any resulting harm, but the maximum per violation and in the aggregate is the same for any level of offense.

Level of Culpability	Penalty "per violation"
• The person did not know (and by exercising reasonable diligence would not have known) that such person violated such provision	* $100 - $50,000 * Maximum Penalty*: $1,500,000
• The violation was due to reasonable cause and not to willful neglect	* for each violation : $1,000 - $50,000 * Maximum Penalty*: $1,500,000
• Violations due to willful neglect that are corrected within 30 days of when the CE knew or should have known of the violation	* for each violation : $10,000 - $50,000 * Maximum Penalty*: $1,500,000
• Violations due to willful neglect that are not corrected within the 30 day period.	* Penalty for each violation : $50,000 * Maximum Penalty*: $1,500,000

* Represents the maximum penalty for all violations of an identical requirement or prohibition in a calendar year

How Many Violations Occurred?

- Arguably, the single most important factor in establishing the final amount of a penalty is the number of violations – how many times was a single provision violated?
- The differentiated penalties are "per violation." For example, if a covered entity commits one violation of a privacy standard through willful neglect, but corrects the violation, it could be subject to a penalty of $10,000 to $50,000 for the single violation.
- Penalties cannot exceed $1.5 million in a calendar year for a series of *identical* violations.
- So, for any level of violation, where the conduct was not corrected, it only takes 30 violations to reach the maximum penalty of $1.5 million for violations of the same provision in a single year. Where, as in many cases, a new violation occurs every day a standard is not met, 30 violations can accrue quickly.

How Many Violations Occurred?

- The Secretary will determine the number of violations of a standard based on the nature of the covered entity's obligation to act or not act under the specific provision that was violated, such as
  - An obligation to act in a certain manner,
  - To act within a certain time, or
  - To act or not act with respect to certain persons.
- In the case of a continuing violation of a provision, a separate violation occurs ***each day*** the covered entity is in violation of the provision.

Mitigating and Aggravating Factors

- In determining the amount of a penalty per violation, the Secretary is required to determine the nature and extent of the violation and the nature and extent of the harm resulting from such violation.
- The Secretary retains the authority to waive penalties for violations that are due to reasonable cause and not willful neglect, to the extent that the payment of the penalty would be excessive relative to the violation.

Affirmative Defenses

- For violations occurring on or after February 18, 2009, a covered entity has the opportunity to avoid penalties by establishing that an affirmative defense exists, including the following:
  - The violation is an act punishable under 42 U.S.C. 1320d–6*;
  - The violation is not due to willful neglect; and corrected
    - Either during the 30-day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or
    - Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

*Interim final rule in C.F.R. does not reflect statutory change effective 2/18/2011 that would eliminate this affirmative defense in the absence of actual prosecution.

Investigations: A Summary

- From the compliance date to the present, the issues investigated most, in order of frequency:
  - Impermissible uses and disclosures of protected health information;
  - Lack of safeguards of protected health information;
  - Lack of patient access to their protected health information;
  - Uses or disclosures of more than the minimum necessary protected health information; and
  - Complaints to the covered entity.

Cignet

- October 20, 2010 – OCR found that Cignet violated 41 patients' rights by denying them access to their medical records when requested.
- During OCR's investigations of the patients' complaints, Cignet did not respond to OCR's demands to produce records and failed to cooperate with OCR's investigations.
- OCR also found that Cignet's failure to cooperate with OCR's investigations was due to Cignet's willful neglect to comply with the Privacy Rule.

Violation or Breach?

- A violation of HIPAA is not the same thing as a "breach" under HITECH.
- Penalties are assessed for a "violation" of a HIPAA standard, not for a "breach" as defined by HITECH.
  - A "violation" arises any time an entity fails to abide by a HIPAA standard.
  - A "breach" occurs in the event of an unauthorized access or use of unsecured PHI, as defined by the rule.
- Many breaches will involve a "violation" of a HIPAA standard (e.g., failure to maintain security standards or to observe the minimum necessary standard), but a "violation" could occur even if it does not result in a breach.

Violation or Breach?

- Of the three high profile enforcement actions since 2009, two involved the loss or unauthorized disclosure of PHI – but the other did not.
- As the enforcement action taken against Cignet demonstrates, the violation most likely to give rise to non-breach related enforcement actions is the failure to provide individual access to records.
- Refusal to provide access consistent with the Privacy Rule is consistently in the top three position for complaints received by the agency over the last eight years.

Violation or Breach?

- A breach is just the beginning of the problem . . .
- It is a safe assumption that enforcement actions are increasingly likely to be triggered by breaches if for no other reason than the covered entity is now required to self-report breaches, but is not required to report other types of violations.
- Reporting of a breach could thus give rise to an investigation not only of the breach itself, but of the covered entity's (or BA's) overall compliance.
- Breaches will also allow the Secretary to identify recurrent weaknesses and shape industry norms.

Breaches: The Status Quo

- From September 22, 2009 forward, there have been 249 breach reports involving between 500 and 1.7 million persons.
- Location of entity?
  - 44 states, the District of Columbia and Puerto Rico
- Type of entity?
  - Health plans, physicians, hospitals, public and private entities, with 52 involving business associates (who are identified).
- Location of data?
  - 67 laptops, 62 paper records, 36 desktop computers, 36 portable electronic devices, 28 servers, 2 back-up tapes, 2 hard drives, and 2 electronic medical record systems.
- Nature of breach?
  - 140 thefts (laptops predominating), 37 losses (mostly portable devices), 16 hacking or IT incidents (servers and desktop computers), 12 improper disposal (paper records), and 24 unauthorized access.

From Breach . . .*

- Hospital employee removed from the hospital premises documents containing PHI on a Friday afternoon in order to work at home over the weekend. The documents consisted of billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of provider of 66 patients and the practice's daily office schedules for three days containing the names and medical record numbers of 192 patients.
- Monday morning, while commuting to work on the subway, employee placed the documents containing PHI on the seat beside her. The documents were not in an envelope and were bound with a rubber band. Upon exiting the train, employee left the documents on the subway train and they were never recovered.

*Actual incident for which penalty was imposed predated breach reporting requirements.

. . . to Enforcement . . .

- ***Large hospital system to improve policies and procedures safeguarding patient information***
- "The General Hospital Corporation and Massachusetts General Physicians Organization Inc. (Mass General) has agreed to pay the U.S. government $1,000,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the U.S. Department of Health and Human Services (HHS) announced today."

. . . to Corrective Action Plan.

- Adequate policies and procedures governing (i) physical removal and transport of PHI, (ii) laptop encryption, and (iii) USB drive encryption.
- Training: within 30 days of the beginning date of service, certified in writing or in electronic form, including the date training was complete, annually reviewed and updated.
- No removal of PHI from premises for use off-site if workforce member has not completed training.
- Disciplinary action for violations.

Role of Mass General Monitor

- Conduct assessments of implementation and compliance by the covered entity with the CAP:
  - Unannounced site inspections
  - Interview workforce members who use PHI
  - Interview workforce members involved in implementing safeguards required by CAP
  - Inspect sample of laptops and USB flash drives that contain ePHI for compliance
  - Inspect relevant documents

MSO Resolution Agreement

- HHS opened an investigation based on referral from OIG and DOJ, which had been investigating MSO for FCA violations.
- OIG discovered that MSO's owner also owns Washington Practice Management, LLC ("WPM") that earns commissions by marketing and selling Medicare Advantage plans.
- The HHS investigation indicates that the following conduct occurred:
  - Between January 2007 and November 2010, MSO impermissibly disclosed the ePHI it maintained to WPM without a valid authorization, for WPM's purpose of marketing Medicare Advantage plans to those individuals; and
  - MSO intentionally did not have in place appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of the ePHI and did not implement required administrative, physical, and technical safeguards for the ePHI.

Takeaways

- A distinguishing feature of HIPAA/HITECH is that violations do not require "affirmative" wrongdoing – convenience, laziness, and casual "snooping" are potentially big compliance issues:
  - Working at home on weekends
  - Browsing the records of a celebrity
  - Forwarding documents to a personal e-mail address
  - Faxing documents without calling first to verify number
  - Disabling the security features of a laptop or other mobile device
- Culpability levels and number of violations will be influenced by your decisions
  - Failure to train employees
  - Failure to discipline employees who engage in practices that violate HIPAA, or administering discipline in a non-uniform manner based on something other than the seriousness of the infraction
  - Not making "system" upgrades or changes a priority when the status quo is non-compliant
  - Failing to mitigate or avoid harm

Takeaways

- The Secretary has a lot of discretion, and that means any violation can result in substantial penalties
  - Interpretation of statutory language to provide for significant per penalty violations regardless of culpability level
  - Where “per day” is not invoked, Secretary has discretion to determine how many violations occurred
  - Many Privacy Rule violations will have parallel Security Rule violations
  - Secretary has discretion to interpret and apply “mitigating” or “aggravating” factors

Questions?

- Contacts

  Christine Rinn—crinn@crowell.com

  Barbara Ryland—bryland@crowell.com

Reminder—The slides and a link to a recording of the webinar will be sent to attendees.