

# HEALTH LAW

## Update

NEWS FOR THE CLIENTS AND FRIENDS OF BASS, BERRY & SIMS PLC

---

## Enforcing the HIPAA Privacy Rule: Trends, Stats, and Issues

June 11, 2008

The Office for Civil Rights of the Department of Health and Human Services ("OCR") recently released new data regarding enforcement of the HIPAA Privacy Rule.<sup>1</sup> The data include the number of complaints received by OCR, enforcement results, and the top five issues in investigated cases that were closed with corrective action. This Health Law Update briefly summarizes the results of that data.

### **Health Information Privacy Complaints Received**

OCR reports that there were 8,132 health information privacy complaints received during the 2007 calendar year. This information is consistent with a steady trend of increasing complaints over the previous years:

<u>Year</u>	<u>Complaints Received</u>
2007	8,132
2006	7,332
2005	6,853
2004	6,534
2003*	3,744

\* Partial Calendar Year 2003: April 14, 2003 through December 31, 2003

### **Enforcement Results**

OCR resolved 7,176 complaints of privacy violations during the 2007 calendar year. Most of those cases, i.e., 4,977, were resolved after intake and review without a formal investigation, while the remaining 2,199 cases were resolved after an investigation. Roughly a third of the

---

<sup>1</sup> See OCR's HIPAA Compliance and Enforcement Website, <http://www.hhs.gov/ocr/privacy/enforcement/> (follow "Number of Complaints Received by Year" hyperlink). The HIPAA Privacy Rule is set forth at 45 C.F.R. Parts 160 and 164.

investigated cases found that no violation of the Privacy Rule had occurred, while the other two thirds required corrective action.

The enforcement results of 2007 are consistent with a trend of increasing resolutions over the previous years. Although there were 267 fewer cases that underwent an investigation in 2007 than in 2006, the percentages of those investigated cases that required corrective action or that found no violation were about the same as the percentages from previous years:

<u>Year</u>	<u>Total Resolutions</u>	<u>Resolved After Intake &amp; Review</u>	<u>Corrective Action Required</u>	<u>No Violation</u>
2007	7,176	4,977 (69%)**	1,484 (21%)	715 (10%)
2006	6,467	4,001 (62%)	1,571 (24%)	895 (14%)
2005	5,621	3,818 (68%)	1,161 (21%)	642 (11%)
2004	4,764	3,372 (70%)	1,033 (22%)	359 (8%)
2003*	1,508	1,169 (78%)	260 (17%)	79 (5%)

\* Partial Calendar Year 2003: April 14, 2003 through December 31, 2003

\*\* Approximate percentage of total resolutions per year

## **Top Five Issues in Investigated Cases Closed with Corrective Action for 2007**

### **1. Impermissible Uses and Disclosures**

An organization subject to the Privacy Rule ("covered entity") may not use or disclose protected health information except as permitted by the Privacy Rule.<sup>2</sup> For example, a covered entity may use or disclose protected health information for treatment, payment, or health care operations, or as authorized in writing by the individual who is the subject of the information. OCR may require corrective action when a covered entity uses or discloses a patient's information in violation of the Privacy Rule.<sup>3</sup>

#### *Case Example From OCR's Files*

A nurse practitioner who had privileges at a multi-hospital health care system and who was part of the system's organized health care arrangement impermissibly accessed the medical records of her ex-husband. In order to resolve this matter to OCR's satisfaction and to prevent a recurrence, the covered entity: terminated the nurse practitioner's access to its electronic records system; reported the nurse

<sup>2</sup> 45 C.F.R. § 164.502(a). A covered entity must disclose protected health information (a) to an individual when requested, or (b) when required by HHS to investigate or determine the covered entity's compliance with the Privacy Rule. 45 C.F.R. § 164.502(a)(2).

<sup>3</sup> A covered entity that impermissibly uses or discloses protected health information may face other exposure, such as civil penalties and referral of the case to the Department of Justice ("DOJ") for possible criminal penalties. See 45 C.F.R. § 160 Subpart C.

practitioner's conduct to the appropriate licensing authority; and, provided the nurse practitioner with remedial Privacy Rule training.<sup>4</sup>

## 2. Safeguards

A covered entity must have in place appropriate administrative, technical, and physical safeguards to prevent any impermissible use or disclosure of protected health information.<sup>5</sup> Where a use or disclosure of protected health information is permitted, a covered entity must have reasonable safeguards that limit the incidental uses or disclosures of that information.<sup>6</sup> There are a variety of reasonable safeguards that a covered entity may take, depending on factors such as the entity's size and business.<sup>7</sup>

### *Case Example From OCR's Files*

A grocery store based pharmacy chain maintained pseudoephedrine log books containing protected health information in a manner so that individual protected health information was visible to the public at the pharmacy counter. Initially, the pharmacy chain refused to acknowledge that the log books contained protected health information. 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 of all staff on the revised policy. The chain acknowledged that log books contained protected health information and implemented the required changes.<sup>8</sup>

## 3. Access

Except in certain circumstances, individuals have the right of access to inspect and obtain a copy of their protected health information from the records maintained by or for the covered entity.<sup>9</sup>

### *Case Example From OCR's Files*

At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule.

---

<sup>4</sup> <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html#case18>

<sup>5</sup> 45 C.F.R. § 164.530(c).

<sup>6</sup> 45 C.F.R. § 164.530(c)(2).

<sup>7</sup> OCR INCIDENTAL USES AND DISCLOSURES GUIDANCE 1, <http://www.hhs.gov/ocr/hipaa/guidelines/incidentalud.pdf>.

<sup>8</sup> <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html#case1>

<sup>9</sup> 45 C.F.R. § 164.524(a)(1). The Privacy Rule does not extend an individual's right of access to the following: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act ("CLIA") prohibits access, or information held by certain research laboratories. OCR SUMMARY OF THE HIPAA PRIVACY RULE 12, <http://www.hhs.gov/ocr/privacysummary.pdf>; see 45 C.F.R. § 164.524(a)(1)(i)–(iii). Even where the individual has a right of access, a covered entity may deny access in some situations, such as when access to the information may cause harm to the individual or to another. See 45 C.F.R. § 164.524(a)(2)–(3).

Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.<sup>10</sup>

#### 4. Minimum Necessary

With a few exceptions, a covered entity must make reasonable efforts to limit its use and disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.<sup>11</sup> A covered entity may not use, disclose, or request an entire medical record unless there is a specific and justifiable need to do so.<sup>12</sup>

##### *Case Example From OCR's Files*

An OCR investigation confirmed allegations that a dental practice flagged some of its medical records with a red sticker with the word "AIDS" on the outside cover, and that records were handled so that other patients and staff without need to know could read the sticker. When notified of the complaint filed with OCR, the dental practice immediately removed the red AIDS sticker from the complainant's file. To resolve this matter, OCR also required the practice to revise its policies and operating procedures and to move medical alert stickers to the inside cover of the records. Further, the covered entity's Privacy Officer and other representatives met with the patient and apologized, and followed the meeting with a written apology.<sup>13</sup>

#### 5. Notice

Individuals have the right to be informed of the privacy practices of their health plans and health care providers and to be informed of their privacy rights with respect to protected health information.<sup>14</sup> Thus, most covered entities must provide individuals with adequate notice of these rights and practices.<sup>15</sup> Also, some of the exceptions to the Privacy Rule require covered entities to provide or make reasonable efforts to provide a notice to the applicable individual or

---

<sup>10</sup> <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html#case9>

<sup>11</sup> 45 C.F.R. §§ 164.502(b)(1), 164.514(d)(2)–(4). Exceptions to the minimum necessary standard does not apply to the following:

- 1) Disclosures to or requests by a health care provider for treatment purposes;
- 2) Disclosures to the individual who is the subject of the information; and
- 3) Uses or disclosures made pursuant to an individual's authorization.

<sup>12</sup> 45 C.F.R. § 164.514(d)(5).

<sup>13</sup> <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html#case15>

<sup>14</sup> OCR NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION 1, <http://www.hhs.gov/ocr/hipaa/guidelines/notice.pdf> (citing 45 C.F.R. § 164.520).

<sup>15</sup> See 45 C.F.R. § 164.520(b). The notice requirement does not apply to certain health care clearinghouses, correctional institutions, and fully insured group health plans.

take other protective measures as a condition of making a disclosure.<sup>16</sup> For the first time in five years, notice is one of the top five issues in cases closed with corrective action.<sup>17</sup>

#### *Case Example From OCR's Files*

A public hospital, in response to a subpoena (not accompanied by a court order), impermissibly disclosed the protected health information (PHI) of one of its patients. Contrary to the Privacy Rule protections for information sought for administrative or judicial proceedings, the hospital failed to determine that reasonable efforts had been made to insure that the individual whose PHI was being sought received notice of the request and/or failed to receive satisfactory assurance that the party seeking the information made reasonable efforts to secure a qualified protective order. Among other corrective actions to remedy this situation, OCR required that the hospital revise its subpoena processing procedures. Under the revised process, if a subpoena is received that does not meet the requirements of the Privacy Rule, the information is not disclosed; instead, the hospital contacts the party seeking the subpoena and the requirements of the Privacy Rule are explained. The hospital also trained relevant staff members on the new procedures.<sup>18</sup>

#### **Conclusion**

The trends, statistics, and issues for enforcing the HIPAA Privacy Rule in 2007 are consistent with those of previous years. For each year that the number of complaints received by OCR has increased, so has the number of resolutions. Moreover, four of the top five issues that required corrective action in 2007 have been among the top issues since 2003. These trends and issues are important to monitor as the enforcement of the Privacy Rule becomes more prevalent. If you have any questions on the topics covered in this Health Law Update, please contact any of the attorneys in our Healthcare Industry Practice Area listed on the following page.

---

<sup>16</sup> See 45 C.F.R. § 164.512(c)(2) (certain disclosures about victims of abuse) and 45 C.F.R. § 164.512(e)(1) (disclosures pursuant to a subpoena or other discovery request).

<sup>17</sup> See <http://www.hhs.gov/ocr/privacy/enforcement/> (follow "Top 5 Issues in Investigated Cases by Year" hyperlink) (noting that Training, Mitigation, and Complaints to Continuing Education (CE) were among the top five issues in previous years).

<sup>18</sup> <http://www.hhs.gov/ocr/privacy/enforcement/allcases.html#case10>

Bass, Berry & Sims Healthcare Attorneys

**H. Stanford Adams, Jr.**  
(615) 742-7775  
[sadams@bassberry.com](mailto:sadams@bassberry.com)

**Starr Brown**  
(615) 742-6530  
[sbrown@bassberry.com](mailto:sbrown@bassberry.com)

**Pooneh Ghiassi**  
(615) 742-7782  
[pghiassi@bassberry.com](mailto:pghiassi@bassberry.com)

**Angela Humphreys**  
(615) 742-7852  
[ahumphreys@bassberry.com](mailto:ahumphreys@bassberry.com)

**Seth A. Killingbeck**  
(615) 742-7707  
[skillingbeck@bassberry.com](mailto:skillingbeck@bassberry.com)

**Claire F. Miley**  
(615) 742-7847  
[cmiley@bassberry.com](mailto:cmiley@bassberry.com)

**Shannon Pinkston**  
(615) 742-7727  
[spinkston@bassberry.com](mailto:spinkston@bassberry.com)

**Scott B. Shanker**  
(901) 543-5932  
[sshanker@bassberry.com](mailto:sshanker@bassberry.com)

**Krista L. Thornton**  
(615) 742-7734  
[kthornton@bassberry.com](mailto:kthornton@bassberry.com)

**H. Lee Barfield, II**  
(615) 742-6202  
[lbarfield@bassberry.com](mailto:lbarfield@bassberry.com)

**Mary Beth Fortugno**  
(615) 742-7739  
[mfortugno@bassberry.com](mailto:mfortugno@bassberry.com)

**Anna Grizzle**  
(615) 742-7732  
[agrizzle@bassberry.com](mailto:agrizzle@bassberry.com)

**Clevonne M. Jacobs**  
(615) 742-7769  
[vjacobs@bassberry.com](mailto:vjacobs@bassberry.com)

**David King**  
(615) 742-7890  
[dking@bassberry.com](mailto:dking@bassberry.com)

**T. Scott Noonan, Co-Chair**  
(615) 742-6273  
[tnoonan@bassberry.com](mailto:tnoonan@bassberry.com)

**Cynthia Y. Reisz**  
(615) 742-6283  
[creisz@bassberry.com](mailto:creisz@bassberry.com)

**Catherine J.B. Sloan**  
(615) 742-7789  
[csloan@bassberry.com](mailto:csloan@bassberry.com)

**Leigh Walton, Co-Chair**  
(615) 742-6201  
[lwalton@bassberry.com](mailto:lwalton@bassberry.com)

**Philip F. Berg**  
(615) 742-7908  
[pberg@bassberry.com](mailto:pberg@bassberry.com)

**Valere B. Fulwider**  
(615) 742-7742  
[vfulwider@bassberry.com](mailto:vfulwider@bassberry.com)

**Elisa E. Harris**  
(615) 742-6553  
[eharris@bassberry.com](mailto:eharris@bassberry.com)

**J. James Jenkins, Jr.**  
(615) 742-6236  
[jjenkins@bassberry.com](mailto:jjenkins@bassberry.com)

**Leslie Maclellan**  
(615) 742-7818  
[lmaclellan@bassberry.com](mailto:lmaclellan@bassberry.com)

**Brenda N. Phillips**  
(615) 742-6237  
[bnphillips@bassberry.com](mailto:bnphillips@bassberry.com)

**Brian D. Roark**  
(615) 742-7753  
[broark@bassberry.com](mailto:broark@bassberry.com)

**Danielle M. Sloane**  
(615) 742-7763  
[dsloane@bassberry.com](mailto:dsloane@bassberry.com)

**Elizabeth S. Warren**  
(615) 742-7719  
[ewarren@bassberry.com](mailto:ewarren@bassberry.com)

*The materials contained herein have been abridged from the statutory sources and should not be construed or relied upon for legal advice. Readers are urged to consult legal counsel concerning particular situations and specific legal questions.*

*To ensure compliance with requirements imposed by the IRS, we inform you that this message is not intended to be used, and cannot be used, by the addressee or any other person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.*