

## The HIPAA Privacy Rule

### **What is the HIPAA Privacy Rule?**

The *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule) came into effect on April 14, 2001. The rule creates national standards to protect individuals' personal health information and gives patients increased access to their own medical records. The mandate for the Privacy Rule comes from the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191.<sup>1</sup> In response to the HIPAA mandate, the Department of Health and Human Services (HHS) published a final regulation in the form of the Privacy Rule in December 2000. The rule was corrected in February 2001, and then final modifications were adopted in August 2002.

### **What is the purpose of the HIPAA Privacy Rule?**

Congress articulated the purpose of the privacy rule as follows:

- ▶ to improve the Medicare and medicaid programs;
- ▶ to improve the efficiency and effectiveness of the health care system;
- ▶ to encourage the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.<sup>2</sup>

### **Who is charged with observing the Privacy Rule?**

The privacy rule applies to the following kinds of providers:

- ▶ health care **plans**<sup>3</sup>;
- ▶ health care **clearinghouses**;
- ▶ health care **providers** who conduct certain financial and administrative transactions electronically.<sup>4</sup>

Most covered entities were to have complied with the Privacy Rule by implementing standards to protect and guard against the misuse of individually identifiable health information by April 14, 2003. Small health care plans have until April 14, 2004 to comply.<sup>5</sup> Under certain circumstances, if covered entities fail to implement standards to comply with the Privacy Rule in a timely manner, civil or criminal penalties may apply.<sup>6</sup>

### **What is Protected Health Information (PHI) under the Privacy Rule?**

Protected Health Information (PHI) is what the Privacy Rule protects. Under the HHS regulations, PHI includes any Individually Identifiable health information regarding a person's physical or mental health. Individually Identifiable Health Information is Health Information that identifies an individual *or* provides a reasonable basis to believe that it can be used to identify an individual.<sup>7</sup>

Health Information under HIPAA means any information, whether oral or recorded in any medium that:

- is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; *and*
- relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.<sup>8</sup>

### **What sorts of disclosures of PHI are permitted under the Privacy Rule?**

Disclosure of PHI is permitted<sup>9</sup> for the following purposes (often remembered as "TPO"):

- **Treatment** of the patient;
- **Payment**;
- health care **Operations**.

With some important exceptions, a covered entity may disclose PHI **to a business associate** and may allow the business associate to create or receive PHI on its behalf, so long as the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the PHI.<sup>10</sup>

In addition, the final rule provides that uses or disclosures of PHI that are **incidental to an otherwise permitted use or disclosure** may occur, provided that the covered entity has met the reasonable safeguards and minimum necessary requirements of the rule. Incidental uses or disclosures under these circumstances might include, for example, physician waiting room sign-in sheets; patient charts maintained at bedside in hospitals; physicians' conversations with patients in semi-private rooms; or physicians' conversations at nurses' stations.<sup>11</sup>

### **Under what additional circumstances may PHI be disclosed?**

The following additional disclosures of PHI are permitted by HIPAA:

- **De-identified Information** - Health information can be used if sufficiently altered so that the persons to whom it refers are no longer individually identifiable.<sup>12</sup>
- **Limited Data Set and Limited Data Use Agreement** - The final rule permits the creation and dissemination of a limited data set that does not include any individually identifiable information for research, public health, and health care operations *provided that* the user agrees to use the information only for the specific purpose for which the information is given.<sup>13</sup>
- **Research** - Researchers, with proper approval, may use PHI in studies so long as they review only the PHI necessary to their research.<sup>14</sup>
- **Deceased Persons** - PHI regarding deceased persons may be used for public health, forensic and funerary purposes.<sup>15</sup>
- **"Grandfathered" Research** - Research that began before April 14, 2003 will not generally be affected by the new rule.<sup>16</sup>
- **As Required by Other Law** for the following:

- ▶ **Public Health Purposes** - the collection of information for epidemiological and other public health purposes, including regulation and oversight by the FDA.<sup>17</sup>
- ▶ **For Victims** - relating to cases of abuse, neglect or domestic violence.<sup>18</sup>
- ▶ **Use by Judicial or Administrative Courts** - to comply with court orders; or subpoenas, discovery requests or other lawful process, in some cases.<sup>19</sup>

### **What sorts of disclosures of PHI require patient *authorization*?**

*Authorization* under the Privacy Rule is required for uses and disclosures of health information that is not otherwise to be disclosed for purposes of TPO or other permitted purposes (A common example is health information used for marketing activities.).<sup>20</sup> PHI can be released if a patient has authorized its use for a specified purpose. Patients will have to grant permission in advance for each type of non-routine use or disclosure they choose to authorize.<sup>21</sup> Patients may revoke these authorizations at any time by so requesting in writing.<sup>22</sup>

### **Does HIPAA preempt Pennsylvania law?**

HIPAA will preempt state laws that are in *conflict* with its regulatory requirements, with the exception of certain public health and related laws.<sup>23</sup> HIPAA's confidentiality protections, however, are cumulative. HIPAA's privacy rule sets a "floor" of privacy standards rather than a "ceiling." State laws with more restrictive protections will continue to apply.<sup>24</sup>

### **Do more restrictive privacy protections continue to apply under Pennsylvania law?**

Stronger state privacy laws, such as those provided in Pennsylvania Act 148 (1998), continue to apply because HIPAA does not preempt "more stringent" state privacy protections.<sup>25</sup> Many HIV-positive persons in Pennsylvania already receive privacy notices, similar to the notices they will see under HIPAA, pursuant to Pennsylvania Act 148. The privacy protections of HIPAA and Act 148 will be cumulative.

### **Are there penalties for violating HIPAA?**

HIPAA provides that HHS may impose nominal penalties of not more than \$100 per violation for failure to comply with the Privacy Rule.<sup>26</sup>

The statute also establishes the offense of Wrongful Disclosure of Individually Identifiable Health Information. The offense is punishable by up to a \$50,000 fine and/or a year in prison. A \$100,000 fine and/or 5 years in prison may be applied if the offense is committed *under false pretenses*; and a \$250,000 fine and/or 10 years in prison may be applied if the offense is committed *with intent to sell, transfer or use* individually identifiable health information *for commercial advantage, personal gain or malicious harm*. The following elements are required to establish wrongful disclosure of individually identifiable health information:

A person must (1) knowingly;  
(2) do one or more of the following:  
(a) *use or cause to be used* a unique health identifier;  
(b) *obtain* individually identifiable health information relating to an individual;  
(c) *disclose* individually identifiable health information to another person.<sup>27</sup>

### **How is HIPAA likely to affect people living with HIV/AIDS in Pennsylvania?**

Although clients with HIV and AIDS usually already see privacy notices and authorization forms pursuant to Pennsylvania Act 148, clients may see more or slightly different notices and authorizations as health care plans, clearinghouses and providers bring their documents and protocols into compliance with the national standards established by HIPAA.

HIPAA will likely have the following consequences:

- ▶ Health care consumers, in the aggregate, will enjoy greater privacy protections regulating how health information is handled.
- ▶ HIPAA's requirements will mean that required authorizations for releases of records will become more common within the health care community as a whole.
- ▶ The additional administrative burdens involved for the required new authorizations may slow the transmission of patient information.

### **Where can more specific information about HIPAA be found?**

HIPAA Statute (re Privacy Rule): <http://aspe.hhs.gov/admnsimp/pl104191.htm>

HIPAA Privacy Regulations: <http://www.hhs.gov/ocr/hipaa/finalreg.html>

HHS Information: [www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/)

CDC Information: <http://www.cdc.gov/privacyrule/>

NIH Information: <http://privacyruleandresearch.nih.gov/>

Information specific to Pennsylvania: [www.dpw.state.pa.us/omap/hipaa/omaphipaa.asp](http://www.dpw.state.pa.us/omap/hipaa/omaphipaa.asp)

The Health Privacy Project: <http://www.healthprivacy.org>

## NOTES

1. *See* Health Insurance Portability and Accountability Act of 1996, Sec. 264, P.L. 104-191 (August 21, 1996).
2. *See id.* at Sec. 261.
3. Significantly, the Act defines "health plan" as "an individual or group plan that provides, or pays the cost of, medical care." "Health plan" includes the following and any combination thereof: a group health plan that has 50 or more participants or is administered by an entity other than the employer who established and maintains the plan; a health insurance provider; a health maintenance organization; Medicare Part A or B; medicaid; a Medicare supplemental policy; a long-term care policy; an employee welfare benefit plan or similar arrangement; the health care program for active military personnel; the veterans health care program; the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); the Indian health service program; and the Federal Employees Health Benefit Plan. *See* Health Insurance Portability and Accountability Act of 1996, Sec. 1171 (5), P.L. 104-191 (August 21, 1996).
4. *See* 45 CFR 160.101.
5. The Act leaves discretion to the Secretary of HHS to determine the meaning of "small health plans" for compliance purposes. *See* Health Insurance Portability and Accountability Act of 1996, Sec. 1175 (b)(1)(B), P.L. 104-191 (August 21, 1996). Accordingly, the Regulations establish that a small health plan means "a health plan with annual receipts of \$5 million or less." *See* 45 CFR 160.103.
6. *See* Health Insurance Portability and Accountability Act of 1996, Sec. 1176, 1177, P.L. 104-191 (August 21, 1996).
7. *See id.* at Sec. 1171 (6).
8. *See id.* at Sec. 1171 (4).
9. Although the initial version of the privacy rule promulgated by HHS *required* providers to obtain a general patient consent for the disclosure of TPO information, the final rule removes the mandatory consent requirements. The final rule merely requires covered entities to provide patients with notice of the patients' privacy rights and the covered entities' privacy practices. Direct treatment providers are required to make a good-faith effort to obtain patients' written acknowledgment of the notice of privacy rights and practices. *See* 45 CFR 164.506. *See also* HHS Press Release (August 9, 2002): <http://www.hhs.gov/news/press/2002pres/20020809.html>.
10. *See* 45 CFR 164.502 (e).
11. *See* 45 CFR 164.502 (a)(1)(iii). *See also* HHS Press Release (August 9, 2002): <http://www.hhs.gov/news/press/2002pres/20020809.html>.

12. See 45 CFR 164.514 (a) and (b).
13. See 45 CFR 164.514 (e).
14. See 45 CFR 164.512 (i).
15. See 45 CFR 164.512 (g).
16. See 45 CFR 164.532(c).
17. See 45 CFR 164.512(b).
18. See 45 CFR 164.512(c).
19. See 45 CFR 164.512(e).
20. See 45 CFR 164.508 (a)(3). But note here that face-to-face communications with patients about treatment options or about a health care entity's own available products or services (or promotional gifts) is not considered "marketing" for the purposes of this part. See 45 CFR 164.508 (a)(3)(A) and (B).
21. See 45 CFR 164.508 (a)(1).
22. See 45 CFR 164.508 (b)(5).
23. The updated 45 CFR 160.203(c) provides that state law is not preempted by the HIPAA Privacy Rule if "the provision of the State law, including procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention."
24. See Health Insurance Portability and Accountability Act of 1996, Sec. 264 (c)(2) and 1178, P.L. 104-191 (August 21, 1996).
25. See Health Insurance Portability and Accountability Act of 1996, Sec. 264, P.L. 104-191 (August 21, 1996). The *Regulation* defines "more stringent" protections, as applied here, as those that "increase the privacy protections afforded (such as by expanding the criteria for) or reduce the coercive effect of the circumstances surrounding the express legal permission." 45 CFR 160.202 (4).
26. See Health Insurance Portability and Accountability Act of 1996, Sec. 1176 (1), P.L. 104-191 (August 21, 1996).
27. See Health Insurance Portability and Accountability Act of 1996, Sec. 1177, P.L. 104-191 (August 21, 1996).