

**Email**

healthcareinfo@mosessinger.com

**Web Site**www.mosessinger.com  
www.ehealthlawtoday.com

This periodic newsletter is written by the Healthcare Practice Group at Moses & Singer to help healthcare professionals navigate the rapidly changing law in the healthcare industry.

**Background**

On November 3, 1999, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") were published in the Federal Register<sup>1</sup> (the comment period closed on February 17, 2000, but the Privacy Rule has not yet been finalized). The Privacy Rule seeks to protect the privacy of individually identifiable health information, or "protected health information" ("PHI").<sup>2</sup> The Privacy Rule would require certain "Covered Entities"<sup>3</sup> to comply with specific measures and to take precautions to protect the privacy of an individual's healthcare information which is or has been electronically maintained or transmitted. Although the Privacy Rule is not yet final, given the extensive nature of the compliance requirements it will place on Covered Entities, we offer this summary to help organizations plan for the future. We will amend this Advisor when the Privacy Rule is final.

# Healthcare Law

# Advisor

February 2000 Vol. 2 No. 2

## Compliance by Covered Entities with the Proposed Privacy Rule Protecting Individually Identifiable Health Information

With respect to compliance issues, the Privacy Rule is divided into essentially three categories: (A) rights of individuals; (B) the structure of a compliance program; and (C) compliance reviews, records and enforcement.

**A. Rights of individuals**

A Covered Entity will be required to develop policies and procedures for the following:

1. **notifying individuals of its practices** with respect to PHI with sufficient detail to put individuals on notice of expected uses and disclosures of PHI, which such notice must include specific language and must be distributed by **health plans** at the following times:
  - by the date the health plan is required to be in compliance with the final Privacy Rule,
  - at enrollment,
  - within 60 days of a material change to the practices, and
  - once every three years

**Providers** must give such notification to individuals who are being served at the time of first service delivery within a year of the date the provider is required to be in compliance with the final Privacy Rule AND providers must post the notice in a clear and prominent place for individuals to read the notice as well as have copies available for individuals to take with them;<sup>4</sup>

2. **granting individuals access** to their PHI for the entire time that the Covered Entity maintains such information;<sup>5</sup>
3. **keeping records of all disclosures** of PHI and accounting to individuals for disclosures of their PHI, including disclosures authorized by the individual, and providing the date of each disclosure, the name and address of the person or organization to whom the disclosure was made and a description of the information released;<sup>6</sup> and
4. **granting individuals the right to amend and correct** their PHI and apprising individuals of such right, including informing individuals when

their amendments and corrections have been accepted and apprising relevant parties of such changes, including Business Partners,<sup>7</sup> as well as notifying individuals when their amendments and corrections have not been accepted.<sup>8</sup>

**B. Structure of a Compliance Program.**

Significant administrative requirements in structuring a compliance program with which a Covered Entity will be required to comply include, but are not limited to, the following:

1. A Covered Entity will be required to document its policies and procedures with respect to PHI, distinguishing between permitted disclosures and disclosures required by law (including any violation of such procedures or amendments thereto);<sup>9</sup> such policies and procedures include, but are not limited to, the following:
  - uses and disclosures by the Covered Entity or its Business Partners;
  - disclosures to individuals, including how notices will be disseminated, and procedures for accepting or denying requests;
  - procedures for training employees, receiving complaints, imposing sanctions, and mitigation of harm; and
  - implementation of changes in policies or procedures.<sup>10</sup>
2. A Covered Entity must also do the following:
  - **designate a Privacy Official**<sup>11</sup> responsible for developing and implementing the privacy policies and procedures of the Covered Entity;
  - **train all of its staff** who are in contact with PHI about use and disclosure of PHI by the date on which the Privacy Rule becomes applicable to the Covered Entity;
  - **implement sanctions** for employees' violation of the Covered Entity's policies and procedures;<sup>12</sup>
  - establish and implement **safeguards** to protect the privacy of PHI;<sup>13</sup>
  - establish and implement a **complaint process**,

**“Although the elements of these administrative requirements resemble the general model of compliance plans in other areas . . . [these compliance requirements] contain important differences.”**

which such process would include designating a contact person to receive complaints and maintaining a record of all complaints received;<sup>14</sup> and

- establish procedures for **mitigating harm** caused by unauthorized disclosures of PHI.<sup>15</sup>

Although elements of these administrative requirements resemble the general model of compliance plans in other areas of health law, such as Medicare + Choice, the subject matter of such compliance is new, the persons involved may be different and components of a compliance program contain important differences. For example, Covered Entities must place sanctions on their employees for failing to comply with the policies and procedures of the Covered Entity or the requirements of the Privacy Rule. Another interesting difference is the duty of the Covered Entity to mitigate any deleterious effect of a use or disclosure of PHI. This particular duty could prove particularly burdensome for the Covered Entity because the duty to mitigate extends to deleterious uses by the Covered Entity's Business Partners.<sup>16</sup> And, the Privacy Rule would preempt State law concerning confidentiality of patient information except in the following three circumstances: (1) State laws that the Secretary of Health and Human Services determines are necessary for certain purposes set forth in the statute; (2) State laws that the Secretary determines address controlled substances; and (3) State laws relating to the privacy of individually identifiable health information that are contrary to and **more stringent than** the federal requirements. (emphasis added).

### C. Compliance, Records and Enforcement

Covered Entities would be required to maintain records as directed by the Secretary of Health and Human Services, and would be required to participate in compliance reviews, including supplying information to the Secretary on demand.<sup>17</sup> Significantly, individuals (including employees acting as whistleblowers) would have the right to file a complaint with the Secretary if they believe that a Covered Entity has failed to comply with the Privacy Rule.<sup>18</sup> The Secretary has discretion as to whether to initiate an action

pursuant to such complaint. The Privacy Rule does not create a private right of action (although State law may create a private right of action for violation of State laws which have not been preempted by this Privacy Rule). Any enforcement action, whether initiated by the Secretary or pursuant to a complaint may result in the imposition of civil monetary penalties of up to \$25,000 for each standard that is violated, per calendar year, and criminal penalties of up to \$250,000 and/or ten years in prison.<sup>19</sup>

#### Endnotes

<sup>1</sup>See 64 Fed. Reg. 59918. The Privacy Rule proposes to amend Title 45 of the C.F.R., Parts 160 through 164. Please note that all references to the CFR are to the proposed regulations.

<sup>2</sup>The Privacy Rule prohibits the use or disclosure of "PHI." "PHI" is defined as "individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form." For purposes of the definition of PHI, "(i) 'Electronically transmitted' includes information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and 'faxback' systems. (ii) 'Electronically maintained' means information stored by a computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media." PHI excludes "(i) [i]ndividually identifiable health information in education records covered by the Family Educational Right and Privacy Act, as amended, and (ii) [i]ndividually identifiable health information of inmates of correctional facilities and detainees in detention facilities." 45 CFR §164.504.

<sup>3</sup>The Privacy Rule indicates that it applies to "Covered Entities" which includes "health plans, health care clearinghouses and health care providers who transmit health information in electronic form." See 45 CFR §160.102. Covered Entities are given twenty-four months from the effective date of the Privacy Rule in which to comply with its requirements. 45 CFR § 164.524.

Covered Entities which are small health plans have thirty-six months from the effective date of the Privacy Rule to comply (a "small health plan" is defined as a health plan with annual receipts of \$5 million or less, see 45 CFR § 160.103).

<sup>4</sup>See 64 Fed. Reg. at 59978, 59979; 45 CFR § 164.512.

<sup>5</sup>See 64 Fed. Reg. at 59983; 45 CFR § 164.514

<sup>6</sup>See 64 Fed. Reg. At 59985-86; 45 CFR § 164.515

<sup>7</sup>A "Business Partner" is defined in the Privacy Rule to mean, with respect to a Covered Entity, "a person to whom the [C]overed [E]ntity discloses PHI so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity." 45 CFR §164.504

<sup>8</sup>See 64 Fed. Reg. at 59987-88; 45 CFR § 164.516

<sup>9</sup>See 64 Fed. Reg. at 59997; 45 CFR § 164.520

<sup>10</sup>See 45 CFR §164.520

<sup>11</sup>45 CFR § 164.518(a)

<sup>12</sup>See 64 Fed. Reg. at 59986-89; 45 CFR § 164.518(b)

<sup>13</sup>45 CFR § 164.518(c)

<sup>14</sup>See 64 Fed. Reg. 59991; 45 CFR § 164.518(d)

<sup>15</sup>See 64 Fed. Reg. at 59991

<sup>16</sup>See 64 Fed. Reg. at 59949 and 59991; *see also* 45 CFR §164.504(e)(2)(iii)—a material breach by a Business Partner will be considered noncompliance by a Covered Entity if the Covered Entity knew or reasonably should have known of the breach and failed to take reasonable steps to cure the breach or terminate the contract.

<sup>17</sup>See 64 Fed. Reg. at 60002; 45 CFR §164.522(d)

<sup>18</sup>See 64 Fed. Reg. at 60002; 45 CFR §§164.518(c), 164.522(b)

<sup>19</sup>See 64 Fed. Reg. at 60003.

This Advisor was written by Jackie Huchenski, Linda Abdel-Malek and Jessica Friedman. If you have any questions about this Advisor or our healthcare practice, please contact Jackie Huchenski, partner and Chair of the Healthcare Practice Group, by telephone at (212) 554-7831 or e-mail at [jhuchenski@mosessinger.com](mailto:jhuchenski@mosessinger.com).

This Bulletin is intended as a general comment on certain recent developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the Firm on the legal issues herein described. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions but that professional advice be sought in connection with any such transaction.