Making Sense of HIPAA Privacy: Solutions for Complex Compliance Dilemmas

Jack A. Rovner
Making Sense of HIPAA Privacy: Solutions for Complex Compliance Dilemmas

Jack A. Rovner*

ABSTRACT: This Article examines and proposes solutions for the following compliance problems under the Health Information Portability and Accountability Act’s Privacy Rule: (a) determining compliance requirements when multiple provisions of the Privacy Rule allow a use or disclosure of protected health information; (b) managing minimum necessary for disclosures to noncovered entities; (c) managing interaction between organized healthcare arrangements and noncovered providers; (d) processing joint health and life/disability insurance applications; (e) reconciling family coverage explanations of benefits and family member’s confidential communication demands; and (f) explaining denial of protected health information access based on endangerment. In the course of the analysis, the Article presents a Privacy Rule Compliance Tool that summarizes the compliance requirements associated with each Privacy Rule provision that allows protected health information use or disclosure.

* Partner and co-chair of the Health Law Practice Group at Neal, Gerber & Eisenberg LLP, Chicago, Illinois. Mr. Rovner received a Bachelor of Arts from Brandeis University in 1968 and a Juris Doctor, cum laude, from Boston University Law School in 1976.


The Privacy Rule Compliance Tool presented in Section I of this Article was conceived by Nicholas S. Harned, J.D., cum laude, 1998, University of Wisconsin Law School and L.L.M., Health Law, 2001, Loyola University Chicago School of Law, an associate with the law firm of Michael Best & Friedrich LLP, while assisting the author with analyzing compliance obligations when multiple Privacy Rule provisions allow protected health information uses and disclosures.
Healthcare providers, health plans, and healthcare clearinghouses required to comply with the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)\(^1\) face complex compli-


Healthcare providers are subject to the HIPAA Administrative Simplification provisions once they transmit, or have transmitted on their behalf, electronic transactions for which the HIPAA Transactions Rule, 45 C.F.R. pt. 162, has set standards. See 42 U.S.C. § 1320d-1(a)(3) (2000); 45 C.F.R. § 160.102(a)(3) (2004). The Transactions Rule sets standards for the following electronic transactions: (a) healthcare claims and equivalent encounter information; (b) healthcare payment and remittance advice; (c) coordination of benefits; (d) healthcare claim status; (e) eligibility for a health plan; (f) referral certification and authorization; (g) enrollment and disenrollment in a health plan; and (h) health plan premium payment. See 45 C.F.R. pt. 162.

All health plans and all healthcare clearinghouses are subject to the HIPAA Administrative Simplification provisions. See 42 U.S.C. §§ 1320d-1(a)(1), 1320d-1(a)(2); 45 C.F.R. §§ 160.102(a)(1), 160.102(a)(2). A healthcare clearinghouse is a public or private entity, such as a billing service, repricing company, or value-added network or switch, that processes or facilitates the processing of health information received from one entity into or out of the transaction standards established by the Transactions Rule for transmission to another entity. See 42 U.S.C. § 1320d(2); 45 C.F.R. § 160.103.

A health plan is a group or individual plan that provides or pays the cost of medical care. See 42 U.S.C. § 1320d(5); 45 C.F.R. § 160.103. The term includes health insurance issuers, health maintenance organizations, and government health benefits programs such as Medicare, Medicaid, the Civilian Health and Medical Program of the Uniformed Services, the Federal Employees Health Benefits Program, the Indian Health Service Program, State children’s health insurance plans, and State health benefits high-risk pools. See 42 U.S.C. § 1320d(5); 45 C.F.R. § 160.103.

All employee welfare benefit plans, as defined in Section 3(1) of Title I of the Employee Retirement Income Security Act of 1974, 29 U.S.C. § 1002(1), that have at least 50 participants or that are administered by entities other than the employers which established and maintain the plans are subject to the HIPAA Administrative Simplification provisions as group health plans. See 42 U.S.C. § 1320d(5)(A); 45 C.F.R. § 160.103.

An employee welfare benefit plan with less than 50 participants that is administered solely by the employer which established and maintains the plan is not subject to the HIPAA Administrative Simplification provisions. Employers, unions, government agencies, church organizations, and other sponsors of group health plans are also not subject to the HIPAA Administrative Simplification provisions. See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,496 (Dec. 28, 2000). The following types of insurance coverage are not subject to the HIPAA Administrative Simplification provisions, even though they may pay medical benefits: life, disability income, workers’ compensation, automobile medical payment, general and automobile liability, credit-only, and nursing home fixed-indemnity. See 45 C.F.R. § 160.103; Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,567.
Complex Compliance

ance dilemmas under the HIPAA Privacy Rule. Among the most vexing is the dilemma of determining compliance requirements when more than one provision of the Privacy Rule allows use or disclosure of protected health information.

Other compliance dilemmas include managing minimum necessary for disclosures of protected health information to payors and providers who are not Covered Entities; managing interaction between organized healthcare arrangements and providers who are not Covered Entities; processing joint applications for health and life/disability insurance; reconciling confidential communication demands with explanation of benefits issuance in family coverage; and balancing the withholding of protected health information on grounds of endangerment with the obligation to explain the basis for denying protected health information access to an individual. This Article proposes solutions to these dilemmas.

2 Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. pt. 164, subpt. E.

3 Protected health information is individually identifiable health information that is maintained or transmitted by covered entities—the healthcare providers, health plans, and healthcare clearinghouses that are subject to the HIPAA Administrative Simplification provisions. See 45 C.F.R. § 160.103; Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,620 (“[P]rotected health information is the subset of individually identifiable health information that is maintained or transmitted by [a] covered entity.”).

Individually identifiable health information is any information, including demographic information collected from an individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or 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, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 U.S.C. § 1320d(6); see 45 C.F.R. § 160.103.

The Privacy Rule does not apply to individually identifiable health information in an employment record or in an educational record subject to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g. See 45 C.F.R. § 160.103. “Use” of protected health information means “sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.” Id. “Disclosure” of protected health information means “release, transfer, provision of, access to, or divulging in any other manner of [such] information outside the entity holding the information.” Id.
I. Multiple Provisions Allowing Use or Disclosure

There are many instances in which more than one Privacy Rule provision will allow use or disclosure of protected health information. For example, a disclosure allowed for a claim collection or subrogation payment activity or a legal services healthcare operation\(^4\) may also be allowed for a judicial proceeding or a health oversight activity.\(^5\) The disclosure for payment or healthcare operations is not accountable to the individual,\(^6\) but it is accountable when made for a judicial proceeding or a health oversight activity.\(^7\) What is the compliance obligation of the Covered Entity making a disclosure that is allowed by multiple Privacy Rule provisions?

This section demonstrates that a Covered Entity need only comply with the requirements of the one Privacy Rule provision upon which it relies to make a use or disclosure of protected health information. It also explains, and provides a Privacy Rule Compliance Tool that summarizes, the compliance requirements associated with each Privacy Rule provision that allows use or disclosure of protected health information.

A. The Privacy Rule Compliance Tool

The Privacy Rule Compliance Tool that follows arrays the Privacy Rule’s compliance requirements for protected health information uses and disclosures. Generally, the higher the level number of the Tool, the greater the compliance requirements associated with the uses and disclosures allowed at that level.

Part B of this section proves the validity of the tool by demonstrating (a) that a covered entity may rely on any one level of the tool that provides a basis for the use or disclosure of protected health information that the Covered Entity wants or needs to make, and (b) that the Covered Entity’s compliance requirements will be those, and only those, set out in the level of the tool upon which the Covered Entity relies, even though other levels (whether higher or lower) may also allow the protected health information to be used or disclosed.

---

\(^5\) See id. §§ 164.512(d), 164.512(e).  
\(^6\) See id. § 164.528(a)(1)(i).  
\(^7\) See id. § 164.528(a)(1).
### Privacy Rule Compliance Tool

<table>
<thead>
<tr>
<th>Level</th>
<th>Type of Use or Disclosure</th>
<th>Compliance Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• With the individual (or the individual’s personal representative) &lt;br&gt;• By authorization</td>
<td>• Verify recipient’s identity and, if not the individual, authority &lt;br&gt;• Comply with applicable requirements of other Privacy Rule provisions (e.g., privacy practices notice content for appointment reminders, treatment alternatives, and health products and services) &lt;br&gt;• No minimum necessary &lt;br&gt;• No disclosure accounting</td>
</tr>
</tbody>
</table>

If the use or disclosure qualifies as one of these types, **STOP**. If not, proceed to Level 2.

<table>
<thead>
<tr>
<th>Level</th>
<th>Type of Use or Disclosure</th>
<th>Compliance Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>• With healthcare providers for treatment</td>
<td>• Verify recipient’s identity and authority &lt;br&gt;• Comply with applicable requirements of other Privacy Rule provisions (e.g., restriction agreement or confidential communication request) &lt;br&gt;• No minimum necessary on disclosures; minimum necessary applies to use &lt;br&gt;• No disclosure accounting</td>
</tr>
</tbody>
</table>

If the use or disclosure qualifies as this type, **STOP**. If not, proceed to Level 3.

<table>
<thead>
<tr>
<th>Level</th>
<th>Type of Use or Disclosure</th>
<th>Compliance Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>• With family, friends, others the individual identifies who are involved in care or payment for healthcare &lt;br&gt;• For disaster relief &lt;br&gt;• For provider facility directory</td>
<td>• Obtain advance agreement, if feasible &lt;br&gt;• Apply professional judgment regarding recipient’s identity and authority &lt;br&gt;• Comply with applicable requirements of other Privacy Rule provisions (e.g., restriction agreement or confidential communication request) &lt;br&gt;• Limit to minimum necessary directly relevant to involvement &lt;br&gt;• No disclosure accounting</td>
</tr>
</tbody>
</table>

If the use or disclosure qualifies as one of these types, **STOP**. If not, proceed to Level 4.
## Privacy Rule Compliance Tool, continued

<table>
<thead>
<tr>
<th>Level</th>
<th>Type of Use or Disclosure</th>
<th>Compliance Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>• For payment&lt;br&gt;• For healthcare operations&lt;br&gt;• For national security or intelligence&lt;br&gt;• With correctional institution or law enforcement regarding persons in lawful custody</td>
<td>• Verify recipient’s identity and authority&lt;br&gt;• Comply with applicable requirements of other Privacy Rule provisions (e.g., legal proceedings or health oversight activity)&lt;br&gt;• Limit to minimum necessary&lt;br&gt;• No disclosure accounting</td>
</tr>
</tbody>
</table>

If the use or disclosure qualifies as one of these types, **STOP**. If not, proceed to Level 5.

<table>
<thead>
<tr>
<th>Level</th>
<th>Type of Use or Disclosure</th>
<th>Compliance Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>• Required by law (including to Department of Health and Human Services for compliance investigation and enforcement)</td>
<td>• Verify recipient’s identity and authority&lt;br&gt;• Comply with applicable requirements of other Privacy Rule provisions (e.g., legal proceedings or law enforcement)&lt;br&gt;• No minimum necessary; limit to relevant requirements of the law&lt;br&gt;• Account for disclosure</td>
</tr>
</tbody>
</table>

If the use or disclosure qualifies as this type, **STOP**. If not, proceed to Level 6.

<table>
<thead>
<tr>
<th>Level</th>
<th>Type of Use or Disclosure</th>
<th>Compliance Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>• For public interest or public benefit activity (except national security or intelligence, or correctional institution or law enforcement regarding persons in lawful custody)</td>
<td>• Verify recipient’s identity and authority&lt;br&gt;• Comply with applicable requirements of other Privacy Rule provisions&lt;br&gt;• Limit to minimum necessary&lt;br&gt;• Account for disclosure</td>
</tr>
</tbody>
</table>
B. Proving the Tool

1. First Principle—Any One Privacy Rule Provision is Enough

The Department of Health and Human Services (DHHS), which issued and enforces the Privacy Rule, acknowledges that “more than one section of [the Privacy Rule] potentially could apply with respect to a covered entity’s potential disclosure of protected health information.”

DHHS instructs that, if any one provision of the Privacy Rule allows a protected health information use or disclosure, a Covered Entity may rely on that provision alone as the basis to use or disclose the protected health information:

“If a situation fits one section of the [Privacy Rule] (for example, § 164.512(j) on serious and imminent threats to health and safety), covered entities may disclose protected health information pursuant to that section, regardless of whether the disclosure also could be made pursuant to another section (e.g., § 164.512(f)[,] regarding disclosure to law enforcement officials).[,]”

Hence, a Covered Entity needs only one Privacy Rule provision that allows a protected health information use or disclosure to be able to use or disclose the protected health information. The Covered Entity need not consider any other Privacy Rule provision that may also allow use or disclosure of the protected health information.

---

8 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,538. The DHHS Centers for Medicare and Medicaid Services (CMS), Program Memorandum 60AB illustrates that a particular disclosure of protected health information may be allowed by multiple Privacy Rule provisions. The Program Memorandum instructs Medicare contractors that claims files, furnished to the DHHS Office of Inspector General “for audit sampling,” are disclosures “permissible under several avenues: as health care operations, as required by law, or as required for the investigation and prevention of fraud and abuse.” DHHS, CMS, Program Memorandum 60AB, Medicare Fee for Service Contractor Guidance on the HIPAA Privacy Rule Transmittal 8 (Transmittal AB-03-034, Change Request 2484) (Feb. 28, 2003), available at www.cms.hhs.gov/manuals/pm_trans/AB03078.pdf (last visited June 22, 2004).

9 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,538; see id at 82,499 (“a covered entity may use or disclose protected health information as permitted by and in accordance with a provision of [the Privacy Rule], regardless of whether that use or disclosure fails to meet the requirements for use or disclosure under another provision of [the Privacy Rule]”).
2. Fundamental Use and Disclosure Rule

Privacy Rule Section 502 sets the fundamental rule for use and disclosure of protected health information: “A covered entity may not use or disclose protected health information, except as permitted or required by” the Privacy Rule or by the enforcement and compliance provisions of the HIPAA Administrative Simplification Rules (that is, 45 C.F.R. part 160, subpart C).  

Privacy Rule Section 502(a) lists each of the protected health information uses and disclosures that the Privacy Rule permits or requires. Each is conditioned on compliance with one or more other Privacy Rule provisions that are referenced in the provisions of Section 502(a) (except use and disclosure with the individual permitted by Section 502(a)(1)(i), which references no other Privacy Rule provision). A Covered Entity, making a protected health information use or disclosure allowed by Section 502(a), must comply with the requirements of the Privacy Rule provisions

10 45 C.F.R. § 164.502(a).
11 Privacy Rule Section 502(a) permits or requires the following protected health information uses and disclosures.

- With the individual to whom the protected health information pertains. Id. §§ 164.502(a)(1)(i), 164.502(a)(2)(i).
- For treatment, payment, or healthcare operations “as permitted by and in compliance with § 164.506.” Id. § 164.502(a)(1)(ii). Included in this category are the special healthcare operations of creating limited data sets, fundraising by a covered entity for itself, and health insurance coverage creation, renewal, or replacement, each “[a]s permitted by and in compliance with,” respectively, Sections 164.514(e), (f) or (g). Id. § 164.502(a)(1)(vi); see id. § 164.501.
- For public interest and public benefit activities “as permitted by and in compliance with” Section 164.512. Id. § 164.502(a)(1)(vi).
- With family, friends, and others identified by an individual, and for provider facility directories, as allowed “[p]ursuant to an agreement under, or as otherwise permitted by, § 164.510.” Id. § 164.502(a)(1)(v).
- Pursuant to authorization “in compliance with” Section 164.508. Id. § 164.502(a)(1)(iv).
- As permitted by and “in compliance with” other provisions of Section 502, such as Section 502(d) regarding de-identification of protected health information, Section 502(e) regarding business associates and plan sponsors, and Section 502(g) regarding personal representatives. Id. § 164.502(a)(1)(vi); see id. §§ 164.502(d), 164.502(e), 164.502(g).
- To DHHS “[w]hen required” under the enforcement and compliance provisions of the HIPAA Administrative Simplification Rules “to investigate or determine the covered entity’s compliance with [the Privacy Rule],” Id. § 164.502(a)(2)(ii); see id. §§ 160.300, 160.302, 160.304, 160.306, 160.308, 160.310, 160.312.
- Those that are incidental to the preceding permitted uses and disclosures if the covered entity complies with all applicable minimum necessary requirements of Sections 164.502(b) and 164.514(d) and with the data safeguard requirements of Section 164.530(c). Id. § 164.502(a)(1)(iii).

12 Id. § 164.502(a)(1).
referenced by the provision of Section 502(a) under which the use or disclosure is being made.\footnote{13}

3. Basic Compliance Obligations

Privacy Rule Section 502 sets various basic compliance obligations applicable to all protected health information uses and disclosures.\footnote{14} Other Privacy Rule provisions, such as Sections 504, 514, 520, and 522, set the implementation specifications\footnote{15} for these basic use and disclosure compliance obligations. The following are basic compliance obligations for protected health information uses and disclosures.

\textit{a) Minimum Necessary}

Section 502(b) identifies the uses and disclosures to which minimum necessary applies and those that are excepted from minimum necessary.\footnote{16} Section 514(d) establishes the implementation specifications for minimum necessary.\footnote{17}

Each protected health information use or disclosure that is not excepted from minimum necessary by Section 502(b)(2) is subject to the minimum necessary limitation of Section 502(b)(1) and the minimum necessary implementation specifications of Section 514(d).\footnote{18}

\textit{b) Restriction and Confidential Communication}

Section 502(c) obligates a Covered Entity to comply with any request for restriction on its use or disclosure of protected health information to which it has agreed in accordance with the implementation specifications of Section 522(a).\footnote{19} Section 502(h) obligates a Covered Entity to comply with any confidential communication demand which it has received that satisfies the implementation specifications of Section 522(b).\footnote{20}

A Covered Entity that agrees to an individual’s restriction request or that receives a qualifying confidential communication demand must comply with it, even though Privacy Rule provisions such as those relating to treatment, payment, or healthcare operations would otherwise allow use or disclosure.

\footnotetext[13]{See id.}
\footnotetext[14]{See id. § 164.502.}
\footnotetext[15]{“Implementation specifications” are the “specific requirements or instructions for implementing a standard.” 45 C.F.R. § 160.103.}
\footnotetext[16]{See id. § 164.502(b).}
\footnotetext[17]{See id. § 164.514(d)(2).}
\footnotetext[18]{See id. §§ 164.502(b)(1), 164.502(b)(2), 164.514(d).}
\footnotetext[19]{See id. § 164.502(c).}
\footnotetext[20]{See id. § 164.502(h).}
c) Privacy Practices Notice Content
Section 502(i) obligates a Covered Entity to use and disclose protected health information consistently with the content of its privacy practices notice.21 Section 520 establishes what that content must be.22

These provisions result, for example, in a Covered Entity being prohibited from using or disclosing protected health information to contact individuals to provide appointment reminders or information about treatment alternatives and other health-related benefits and services, even though such activities are healthcare operations, unless the Covered Entity’s privacy practices notice includes the specific statements required by Section 520(b)(1)(iii)(A) of its intent to engage in such activities.23 Similarly, a health plan may not disclose protected health information to an employer, notwithstanding compliance with Section 504(f), unless the health plan includes in the privacy practices notice the statement required by Section 520(b)(1)(iii)(C) regarding an intent to make such disclosures.24

d) Business Associates and Plan Sponsors
Section 502(e) permits a Business Associate25 to create and receive protected health information to perform functions and activities on a Covered Entity’s behalf, provided the Covered Entity complies with the implementation specifications of Section 504(e).26 Section 502(e) further specifies that the Business Associate requirements

---

21 See id. § 164.502(i).
22 See id. § 164.520.
23 See id. § 164.502(i).
24 See id. § 164.504(f)(3)(iii).
25 A “Business Associate” is a person or organization which, other than as a member of a Covered Entity’s workforce, performs or assist in the performance of a function or activity, on behalf of a Covered Entity or an organized healthcare arrangement in which the Covered Entity participates, that either involves the use or disclosure of individually identifiable health information or is regulated by the HIPAA Administrative Simplification Rules. Id. § 160.103. A “Business Associate” also includes a person or organization which, other than as a member of a Covered Entity’s workforce, provides legal, actuarial, accounting, consulting, data aggregation (as defined in [the Privacy Rule]), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person [or organization].

Id.
26 See id. § 164.502(e)(1)(iii).
will not apply to disclosures by a health plan to a plan sponsor if the implementation specifications of Section 504(f) are met. In other words, Section 502(e) allows a health plan to make disclosures to a sponsor of a group health plan by complying with Section 504(f), rather than treating the plan sponsor as a business associate.

e) **Deceased Individuals, Personal Representatives, Whistleblowers, and Workforce Crime Victims**

Sections 502(f), (g), and (j) establish the compliance obligations for dealing, respectively, with deceased individuals, with an individual’s personal representatives, with whistleblowers, and with workforce members who are crime victims.

f) **De-identified Health Information**

Section 502(d) allows disclosure of protected health information for creating de-identified health information, and establishes the rules for use and disclosure of de-identified health information. Sections 514(a)–(c) set the implementation specifications for creating de-identified health information.

---

27 Id. § 164.502(e)(1)(ii)(B).
28 See id. § 164.504(f).
29 A personal representative is a person legally authorized to make healthcare decisions on an individual's behalf or legally authorized to act on behalf of a deceased individual or the individual’s estate. Id. § 164.502(g). The Privacy Rule defers to state and other law to determine the rights of parents and guardians to access the protected health information of their minor children. See id. § 164.502(g)(3).
30 A Covered Entity’s “workforce” consists of its “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.” Id. § 160.103.
31 Protected health information may be de-identified by either of two methods:

1. Having a statistical expert make a documented determination, by application of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, that “the risk is very small” that the information examined “could be used alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information”;

2. Stripping from the information eighteen specified identifiers of individuals and their relatives, household members, and employers, and having no “actual knowledge” that the information remaining “could be used alone or in combination with other information to identify an individual who is a subject of the information.”

Id. § 164.514(b). De-identified health information is no longer individually identifiable health information and, accordingly, is not covered by the Privacy Rule. See id. § 164.502(d)(2).
g) **Identity and Authority Verification**

Implicit in, though curiously not referenced by, Section 502 is the obligation that before disclosing protected health information a Covered Entity must verify the identity of the person, organization, or public official to whom the disclosure will be made and the authority of that person, organization, or public official to receive the protected health information. Section 514(h) sets the implementation specifications for this implicit compliance obligation.

4. **Specific Compliance Obligations—Individuals (Tool Level 1)**

Privacy Rule Section 502(a)(1)(i) permits use and disclosure with an individual of the individual’s protected health information without condition or reference to other Privacy Rule provisions. Section 502(a)(2)(i) requires disclosure to the individual who requests access to or accounting for the disclosures of the individual’s protected health information in accordance with the implementation specifications of Section 524, for access, and Section 528, for accounting.

Use and disclosure involving the individual under Section 502(a)(1)(i) or Section 502(a)(2)(i) are subject to the basic compliance obligations of the other provisions of Section 502 and to the verification provisions of Section 514(h)(1), as applicable to the situation. For example, the provisions of Section 502(g) are applicable when an individual’s personal representatives are involved because Section 502(g) requires a Covered Entity to “treat a personal representative as the individual for purposes of [the HIPAA Administrative Simplification Rules].” Similar to the provisions of Section 502(i) are applicable if a Covered Entity intends to use or disclose protected health information to provide individuals appointment reminders or information about treatment alternatives or health-related benefits and services. Section 502(i) applies in these circumstances because it requires the covered entity to include the statement specified by Section 520(b)(1)(iii)(A) in its

---

32 See id. § 164.502.
33 See id. § 164.514(h)(2).
34 Id. § 164.502(a)(1)(i).
35 Id. § 164.502(a)(2)(i).
36 See id. §§ 164.502, 164.514(h)(1).
37 Id. § 164.502(g)(1). See supra note 29 for the definition of personal representative.

The Privacy Rule allows a Covered Entity to refuse to recognize a person, whom the Covered Entity reasonably suspects of abuse, neglect, or other endangerment of an individual, to be the individual’s personal representative. Id. § 164.502(g)(5).
privacy practices notice before it may use or disclose protected health information for such purposes.\textsuperscript{38}

On the other hand, neither minimum necessary nor disclosure accounting applies because Sections 502(b) and 528 except uses and disclosures with the individual.\textsuperscript{39} Thus, the minimum necessary and disclosure accounting requirements of the Privacy Rule are, by their own terms, not applicable to uses and disclosures with the individual.

5. Specific Compliance Obligations—Treatment, Payment, and Healthcare Operations (Tool Levels 2 and 4)

Privacy Rule Section 506 details the compliance obligations that apply to protected health information use and disclosure for treatment, payment, or healthcare operations as allowed by Section 502(a)(1)(ii).\textsuperscript{40} Section 506(a) imposes three constraints on such protected health information use and disclosure.

1) Use or disclosure of protected health information for marketing must have authorization or otherwise satisfy the requirements of Section 508(a)(3), notwithstanding that the use or disclosure involves treatment, payment, or healthcare operations.\textsuperscript{41}

2) Use or disclosure of psychotherapy notes\textsuperscript{42} must have authorization or otherwise satisfy the requirements of Section 508(a)(2), even if the use or disclosure is for treatment, payment, or healthcare operations.\textsuperscript{43}

3) Every other use or disclosure of protected health information for treatment, payment, or healthcare operations

\textsuperscript{38} Id. § 164.502(i).
\textsuperscript{39} See id. §§ 164.502(b)(2)(ii), 164.528(a)(1)(ii).
\textsuperscript{40} Id. § 164.506.
\textsuperscript{41} See id. § 164.506(a).
\textsuperscript{42} Psychotherapy notes are “notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.” Id. § 164.501. Information regarding “medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of...[d]iagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date” is, by definition, not part of psychotherapy notes. Id.
\textsuperscript{43} See id. § 164.506(a).
Complex Compliance

must be “consistent with other applicable requirements” of the Privacy Rule.44

The third constraint incorporates, as compliance obligations for a treatment, payment, or healthcare operation use or disclosure, every other Privacy Rule provision that, by its own terms, has requirements that are applicable to the particular use or disclosure being made. Section 506 therefore incorporates each applicable basic compliance obligation and implementation specification of, respectively, Sections 502 and 514, such as minimum necessary as applied to use for treatment and to use or disclosure for payment and healthcare operations45 and verification obligations.46

Section 506 also incorporates, as compliance obligations, the requirements of any Section 512 provision allowing use or disclosure for a public interest or public benefit activity that overlaps a disclosure for treatment, payment, or healthcare operations. The use or disclosure for treatment, payment, or healthcare operations will then be “consistent with” the “other applicable requirements” of the overlapping Section 512 provision.47 Some examples follow.

- A Covered Entity that discloses protected health information for its healthcare operation of conducting legal services or its payment activity of collection, claims adjudication, or subrogation must comply with the requirements of Section 512(e) when the disclosure also involves a response to an order, process, or discovery in a legal proceeding in which the covered entity is a participant.48
- A Covered Entity that discloses protected health information for its healthcare operation of licensing or auditing must comply with the requirements of Section 512(d) when the disclosure also involves a license compliance investigation, examination, or review by a health oversight agency, such as a professional registration agency, licensing authority, or insurance commissioner.49
- A Covered Entity that discloses protected health information for its own or another Covered Entity’s healthcare operations involving performance evaluation or fraud and abuse detection, or payment activities such as justification of charges or review of utilization, medical necessity, or appropriateness of care must comply with the requirements

44 Id.
45 See id. §§ 164.502(b)(1), 164.514(d).
46 See id. § 164.514(h).
47 Id. § 164.506(a).
48 Compare id. §§ 164.506(a), 164.506(c)(1), with id. § 164.512(e).
49 Compare id. §§ 164.506(a), 164.506(c)(1), with id. § 164.512(d).
of Section 512(d) if the disclosure involves a health oversight agency conducting an investigation into healthcare fraud or abuse.\footnote{Compare id. §§ 164.506(a), 164.506(c)(1), 164.506(c)(3), 164.506(c)(4), with id. § 164.512(d). See supra note 8 for a discussion of CMS, Program Memorandum 60AB.}

No disclosure for treatment, payment, or healthcare operations will be subject to accounting under Section 528, notwithstanding that the disclosure may also be permitted by accountable public interest or public benefit activities.\footnote{45 C.F.R. § 164.528(a)(1)(i).} Section 528 excepts disclosures “[t]o carry out treatment, payment, and healthcare operations as provided in § 164.506.”\footnote{Id. § 164.528(a)(1)(i).} Hence, Section 528, by its own terms, contains no applicable requirements with respect to disclosures for treatment, payment, or healthcare operations.

\section*{6. Specific Compliance Obligations—Public Interest and Public Benefit Activities (Tool Levels 4, 5, and 6)}

Privacy Rule Section 512 specifies the compliance obligations that apply to uses and disclosures for public interest and public benefit activities, including those required by law.\footnote{The Privacy Rule allows use or disclosure of protected health information without individuals' permission for public interest and public benefit activities as follows.}

\begin{itemize}
  \item As required by law. \textit{Id.} § 164.512(a). “Required by law” means “a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law.” \textit{Id.} § 164.103.
  \item To public health authorities for their legally authorized functions. \textit{Id.} § 164.512(b)(1)(i).
  \item To persons subject to Food and Drug Administration (FDA) jurisdiction with defined legal responsibilities for FDA-regulated products and activities. \textit{Id.} § 164.512(b)(1)(iii).
  \item To health oversight agencies for their legally authorized duties to oversee the healthcare system or government health benefit programs. \textit{Id.} § 164.512(d).
  \item In connection with judicial and administrative proceedings. \textit{Id.} § 164.512(e).
  \item For law enforcement. \textit{Id.} § 164.512(f).
  \item To avert public health and safety threats (including exposure to communicable disease and prevention of crime). \textit{Id.} §§ 164.512(b)(1)(iv), 164.512(j).
  \item For workplace health and safety. \textit{Id.} § 164.512(b)(1)(v).
  \item For compliance with workers' compensation programs. \textit{Id.} § 164.512(l).
  \item For managing decedents (including for the work of coroners, medical examiners, and funeral directors). \textit{Id.} § 164.512(g).
  \item For organ donation. \textit{Id.} § 164.512(h).
\end{itemize}

\begin{footnotesize}
\footnote{Compare id. §§ 164.506(a), 164.506(c)(1), 164.506(c)(3), 164.506(c)(4), with id. § 164.512(d). See supra note 8 for a discussion of CMS, Program Memorandum 60AB.}
\end{footnotesize}
interest or purpose. They reflect interests “of sufficient national importance or relevance to the needs of the health care system to warrant the use or disclosure of protected health information in the absence of either the individual’s express authorization or a legal duty to make such use or disclosure.”

Unlike Section 506(a), Section 512 does not specify that public interest or public benefit use and disclosure must be consistent with other requirements of the Privacy Rule. Consequently, the only Privacy Rule provisions applicable to uses and disclosures allowed by Section 512 are those that apply by their own terms.

Thus, a Covered Entity making a use or disclosure allowed by Section 512 must comply with the basic compliance obligations of Section 502 and the implementation specifications of Section 514 as applicable to the situation. That includes compliance with minimum necessary, except for disclosures required by law, and with the verification provisions of Section 514(h). Similarly, a covered entity must account for each disclosure made pursuant to Section 512, except those made for national security or intelligence purposes or to correctional institutions or law enforcement regarding persons in lawful custody. In contrast, a Covered Entity’s agreement to a restriction request cannot prevent use or disclosure for a public interest or public benefit activity because Section 522(a) makes such an agreement ineffective.

(See Richard M. Campanelli, Director, DHHS Office for Civil Rights, letter to Susan S. Stuard, Director of Regulatory Affairs, Greater New York Hospital Association 1 (Feb. 28, 2003) (“Many disclosures [allowed by the Privacy Rule] further other important public purposes such as reporting child abuse, injuries due to violence, domestic violence or elder abuse, or responding to court orders.”) (on file with the author).)


See 45 C.F.R. § 164.512.

See id.

See id. §§ 164.502(b)(1), 164.502(b)(2)(v), 164.514(d).

Compare id. § 164.528(a)(1), with id. §§ 164.528(a)(1)(vi), 164.528(a)(1)(vii).
7. Specific Compliance Obligations—
   Family, Friends, Provider Facility Directories
   (Tool Level 3)

Privacy Rule Section 510 specifies the compliance obligations that apply to use and disclosure with an individual’s family members, other relatives, and close friends, as well as with any other person whom an individual identifies, when any of these persons are involved in the individual’s care or payment related to the individual’s healthcare.\(^{62}\) It further specifies the compliance obligations for use and disclosure for notification purposes,\(^{63}\) including in disaster relief situations,\(^{64}\) and with respect to listing individuals in provider facility directories.\(^{65}\)

Section 510 does not reference any other Privacy Rule provision.\(^{66}\) Consequently, only those Privacy Rule provisions that are applicable by their own terms to these uses and disclosures—such as Sections 502(b) and 514(d) on minimum necessary and Section 514(h)(2)(iv) regarding use of professional judgment to verify the identity of the family members, other relatives, close friends, or other persons whom an individual identifies—are applicable to the uses and disclosures permitted by Section 510.\(^{67}\)

Hence, a Covered Entity that agrees to an individual’s request not to disclose protected health information to particular family members, other relatives, or other persons in accordance with Section 522(a) will be prohibited by Section 502(c) from making such disclosures, notwithstanding Section 510(b). On the other hand, disclosures allowed under Section 510 are not accountable because Section 528, by its own terms, excepts them.\(^{68}\)

8. Specific Compliance Obligations—
   Authorization (Tool Level 1)

Privacy Rule Section 508 allows any use or disclosure that an individual permits by a written authorization that complies with the procedural and content requirements of Section 508. Section 508 specifies that an authorization is only needed when no other provision of the Privacy Rule or another HIPAA Administrative

---

\(^{62}\) See id. § 164.510(b)(1)(i).
\(^{63}\) See id. § 164.510(b)(1)(ii).
\(^{64}\) See id. § 164.510(b)(4).
\(^{65}\) See id. § 164.510(a).
\(^{66}\) See id. § 164.510(a).
\(^{67}\) See id. § 164.510.
\(^{68}\) See id. § 164.528(a)(1)(v).
Simplification Rule permits or requires the protected health information to be used or disclosed. A Covered Entity relying on an authorization must use or disclose the protected health information “consistent with such authorization.” In other words, the content of a valid authorization controls the Covered Entity’s compliance obligations when the Covered Entity relies on the authorization to make the use or disclosure.

Use and disclosure pursuant to authorization are not subject to minimum necessary or to disclosure accounting because Sections 502(b) and 528, by their terms, do not apply to authorized uses and disclosures. On the other hand, the Covered Entity remains obligated to verify the identity and authority of a recipient to whom an authorization allows disclosure of protected health information because Section 514(h), by its own terms, applies to “any disclosure permitted by” the Privacy Rule, and nothing in Section 508 nullifies that obligation.

II. Minimum Necessary and Noncovered Payors and Providers

A. Payors Who are Not Covered Entities

The Privacy Rule allows a Covered Entity to disclose the minimum necessary protected health information to noncovered payors, such as workers’ compensation and disability income insurers, to obtain payment for healthcare. Hence, covered healthcare providers may submit claims to and coordinate benefits with workers’ compensation and disability income insurers without authorization or other permission of the individual treated. Similarly, a health plan may disclose an enrollee’s protected health information to a workers’ compensation, disability income, or automobile liability insurer for subrogation or benefits coordination without the enrollee’s authorization or permission. In none of these situations may the Covered Entity rely on the representations of the noncovered payors of the minimum amount of protected health information needed to conduct the payment activity. Instead, the Covered Entity must make the minimum necessary assessment to avoid violation of the Privacy Rule.

69 See id. § 164.508(a)(1).
70 Id. § 164.508(a)(1) (2002); see also id. § 164.502(a)(1)(iv) (2004).
71 Id. §§ 164.502(b)(2)(iii) (2004), 164.528(a)(1)(iv).
72 Id. § 164.514(h)(1) (2004).
73 See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,495. See supra note 1 for a description of the payors not subject to the HIPAA Administrative Simplification Rules.
74 See 45 C.F.R. § 164.514(d)(3).
A Covered Entity faces the dilemma of a noncovered payor demanding, as a condition of payment, more protected health information than the Covered Entity believes appropriate for the payment activity. For example, a workers’ compensation or disability income insurer may decline payment unless it receives the entire medical record from the Covered Entity submitting the claim or coordinating benefits. As the noncovered payor is not subject to the HIPAA Administrative Simplification provisions, it is not constrained by the Privacy Rule from routinely demanding an entire medical record. In contrast, the Covered Entity is constrained by the Privacy Rule from disclosing an entire medical record unless “the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose.”75 Indeed, the Covered Entity may not disclose any part of the medical record that the Covered Entity believes to be more than the minimum necessary for the payment needs of the noncovered payor.

Advance planning and preparation are the tools that a Covered Entity may use to resolve this dilemma. Covered Entities that anticipate submitting claims to or coordinating benefits with noncovered payors should seek and document the justifications of those payors for the protected health information they request. The documentation will be particularly prudent for noncovered payors that demand an entire medical record as a condition of payment. The documentation will evidence the Covered Entity’s effort to make its own assessment of the amount of protected health information reasonably needed to conduct the payment activity.

The documentation, if reflecting reasonable bases for the noncovered payors’ protected health information demands, can support the Covered Entity’s adoption of “standard protocols” for the minimum necessary protected health information to include in claims submitted to noncovered payors with which the covered entity routinely or regularly deals. The documentation can also support the “criteria” for measuring the minimum necessary for other noncovered payors’ protected health information requests for particular claims or benefits coordination. Indeed, having such standard protocols and criteria is a minimum necessary compliance obligation.76 Moreover, they can substantially ease the Covered Entity’s dealings with noncovered payors. The alternative is for the Covered Entity to obtain or to receive from the noncovered payor a compliant authorization from the individual that allows

75 Id. § 164.514(d)(5).
76 See id. § 164.514(d)(3).
the Covered Entity to disclose the protected health information that the noncovered payor demands to make payment.

B. Providers Who are Not Covered Entities

The Privacy Rule allows a Covered Entity to disclose the minimum necessary protected health information to noncovered healthcare providers (that is, providers who have never directly or through a Business Associate conducted an electronic transaction for which the Transactions Rule sets standards) for the latter’s payment activities. For example, a hospital subject to the Privacy Rule may disclose its protected health information about an individual it treated to a physician who is not a Covered Entity and wants to file a paper claim for furnishing healthcare to that individual or to an ambulance company that is not a Covered Entity and wants to submit a paper claim for transporting the individual to the hospital. Similarly, a physician subject to the Privacy Rule may disclose protected health information about patients to a clinical laboratory that is not a Covered Entity and wants to submit a paper claim for the services it supplied to the patients at the physician’s request.

In none of these situations may the Covered Entity hospital or physician rely on the representations of the providers not subject to the Privacy Rule of the minimum amount of protected health information needed for the noncovered providers to conduct their payment activities. Instead, the Covered Entity must make the minimum necessary assessment to avoid violation of the Privacy Rule.

A Covered Entity thus faces a verification obligation to determine whether a healthcare provider requesting protected health information for a payment activity is a Covered Entity before responding to the request. This is because the Covered Entity is allowed to rely on the protected health information request to be for the minimum necessary only when the requester is a Covered Entity. Covered Entities that are likely to receive requests from providers such as members of medical staffs, ambulance services, durable medical equipment dealers, home health agencies, and clinical laboratories should accordingly adopt standard protocols to verify whether such providers are Covered Entities. If they are not, the

77 Id. § 164.506(c)(3) (2004). See supra note 1 for information regarding the transactions, the electronic transmission of which make a healthcare provider a covered entity.
78 See 45 C.F.R. § 164.514(d)(3).
79 Id. § 164.514(h)(1).
80 Id. § 164.514(d)(3)(iii)(B).
Covered Entity must be satisfied, based on its own documented assessment, that the protected health information it discloses to such noncovered providers is the minimum needed to conduct payment activities.\textsuperscript{81} Documenting the assessment is critical proof that the Covered Entity complied with its obligation to make its own minimum necessary determination, rather than impermissibly relying on representations of noncovered providers.

The noncovered provider faces the dilemma of justifying to the Covered Entity’s satisfaction that the protected health information requested is the minimum necessary to get a paper claim paid. A noncovered provider, therefore, should be prepared to present to a Covered Entity sufficient documented evidence to show that the protected health information requested is the minimum needed for the payment activity. In the alternative, the noncovered provider should obtain a compliant authorization from the patient that will allow the Covered Entity to disclose the protected health information specified in the authorization to the noncovered provider for payment.

It is not sufficient for a noncovered provider to represent to the Covered Entity that the payor for which the protected health information is requested is a health plan subject to the Privacy Rule. This is because the Privacy Rule places no constraint on the amount of medical information that a Covered Entity may request from noncovered providers and other noncovered entities.\textsuperscript{82} Hence, a health plan may demand any amount of medical information, including an entire medical record, from a noncovered provider without regard for the minimum necessary limitation.

On the other hand, it should be sufficient if the noncovered provider can demonstrate to the Covered Entity that the amount of protected health information requested is the minimum amount that the health plan requests of covered healthcare providers with similar claims. That is because the health plan is limited by the Privacy Rule to requesting of other Covered Entities only the minimum necessary protected health information for that purpose.\textsuperscript{83} Accordingly, a Covered Entity may rely, if reasonable under the circumstances, on such a protected health information request to be for the minimum necessary.\textsuperscript{84}

\textsuperscript{81} Id. § 164.514(d)(3).
\textsuperscript{82} See id. §§ 164.502(b)(1), 164.514(d)(4)(i).
\textsuperscript{83} See id.
\textsuperscript{84} See id. § 164.514(d)(3)(iii)(B).
III. Organized Healthcare Arrangements and Noncovered Providers

The Privacy Rule allows Covered Entities in an organized healthcare arrangement to share protected health information for the arrangement’s healthcare operations.85 Hence, a covered hospital and the covered physicians on its medical staff may share their respective protected health information for quality assessment and improvement activities, credentialing, licensure, accreditation, medical reviews, fraud and abuse detection, compliance programs, business management and planning, and other operations as relate to their clinically-integrated care setting.86 Similarly, covered providers in an independent practice association, physician-hospital organization, or health maintenance organization (HMO) network may share their respective protected health information for healthcare operations that relate to the quality control, utilization management, or financial risk-sharing activities that make them participants in an organized healthcare arrangement.87

Noncovered providers may not participate in any of these organized healthcare arrangement activities, unless individuals whose protected health information would be disclosed to the noncovered providers have given compliant authorizations. Moreover, although a noncovered provider may, without regard for the Privacy Rule, disclose its individually identifiable health information to the Covered Entity participants in an organized healthcare arrangement, it will be a one-way information flow. Once the Covered

85 Id. § 164.506(c)(5). Section 160.103 defines five kinds of organized healthcare arrangements:

1. A clinically-integrated setting, such as a hospital and its medical staff, where individuals typically receive healthcare from more than one provider;
2. An organized system of healthcare, such as an independent practice association, a physician-hospital organization, and a health maintenance organization (HMO) network, that holds itself out to the public as participating in a joint arrangement and in which the participating Covered Entities jointly engage in utilization management, quality assessment and improvement activities, or risk-sharing payment activities;
3. A group health plan and the health insurer or HMO that insures the plan’s benefits with respect to the insurer’s or HMO’s protected health information that relates to present and past enrollees of the group health plan;
4. All group health plans maintained by the same plan sponsor; and
5. All group health plans maintained by the same plan sponsor and all health insurers and HMOs that insure the plans’ benefits with respect to the insurers’ or HMOs’ protected health information that relates to present and past enrollees of the group health plans.

86 See id. §§ 160.103 (defining “organized health care arrangement”), 164.501 (defining “health care operations”).

87 See id. §§ 160.103 (defining “organized health care arrangement”), 164.501 (defining “health care operations”).
Entity participants receive the noncovered provider’s individual identifiable health information, it will be instantly transformed into protected health information. None of the Covered Entities may then disclose it back to the noncovered provider except as the Privacy Rule may otherwise allow. Consequently, both Covered Entities and noncovered providers face the dilemma that the noncovered providers cannot participate in healthcare operations important to effective healthcare delivery and management in clinically-integrated settings and risk-sharing arrangements.

To avoid Privacy Rule violations, covered entities who believe they are in an organized healthcare arrangement must verify that each other participant is, in fact, a Covered Entity before they may disclose protected health information for the healthcare operations of the organized healthcare arrangement.88 Hence, covered hospitals, independent practice associations, physician-hospital organizations, and HMO networks should adopt verification procedures for Covered Entity status before assigning physicians and other providers to activities of their organized healthcare arrangement that involve sharing protected health information for the healthcare operations of the arrangement. Providers who are not subject to the Privacy Rule cannot be allowed to participate in these activities, unless they become Business Associates of the organized healthcare arrangement.89

IV. Joint Health and Life/Disability Insurance Applications

Many employers offer life and disability benefit plans along with health benefit plans. Joint applications for the life and disability coverage and the health coverage are commonly used to enroll employees and their families in both types of coverage. These joint applications usually contain individually identifiable health informa-

88 See id. § 164.514(h).
89 See id. §§ 160.103 (defining “business associate”), 164.502(e), 164.504(e) (2004). Note that a covered entity participating in an organized health care arrangement that performs a [business associate] function or activity...for or on behalf of such organized health care arrangement, or that provides a [business associate] service...to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

Id. § 160.103.
tion of the employee, of any spouse, and perhaps of any emancipated minors (such as college students) and unemancipated minors.

A Covered Entity, such as a health insurer, is subject to the Privacy Rule in all of its activities, unless it elects hybrid entity status.90 A “hybrid entity” is a Covered Entity with business activities that involve both covered functions and noncovered functions and that makes a written designation of its healthcare components—those that perform its covered functions.91 Its “covered functions” are the activities that “make the [covered] entity a health plan, a health care provider or a health care clearinghouse.”92 Thus, an insurer offering both health coverage and life and disability coverage engages in both covered functions and noncovered functions. Unless that insurer elects hybrid entity status, all individually identifiable health information it creates or receives, whether for its health operations or its life and disability operations, will be protected health information subject to the Privacy Rule.93

Once a health insurer that has not “hybridized” receives a joint application for life/disability coverage and health coverage, the individually identifiable health information on the application is instantly transformed into protected health information. The health insurer may not use that protected health information for or disclose it to the life/disability coverage issuer (even if that issuer is a division or other component of the health insurer itself), unless it has authorizations from the individuals whose individually identifiable health information is on the applications. If a broker or insurance agent receives the applications as the Business Associate of the health insurer, the individually identifiable health information on the applications will be instantly transformed into the health insurer’s protected health information, and the broker or agent will be prohibited by its Business Associate Contract from using the protected health information for or disclosing it to the life/disability coverage issuer.94

Processors of joint applications thus face a dilemma. One solution is for the applications to be first submitted to the life/disability insurer if it is independent of the health insurer, or to brokers or agents in their capacity as representatives of an independent life/disability insurer because the brokers or agents may then submit

91 45 C.F.R. § 164.103.
92 Id. § 164.103.
93 See id. § 164.105(a).
94 See id. § 164.504(e).
the applications to the life/disability insurer without regard for the Privacy Rule. The life/disability insurer may extract the individually identifiable health information needed from the applications to underwrite and issue the coverage, then turn the applications or the information over to the health insurance issuer. This solution is not always practical, as the principal coverage sought by these applications is usually health, not life and disability. In addition, the health insurer often provides a variety of services for the life/disability issuer, such as underwriting and premium billing, that may necessitate the health insurer’s use and disclosure of the individually identifiable health information on the applications on the life/disability insurer’s behalf.

Another solution is to obtain Privacy Rule compliant authorizations from the applicants that permit the health insurer to use the individually identifiable health information on the applications for and disclose it to the life/disability issuer even though it becomes protected health information when the health insurer receives it. This solution expands the burdens of the enrollment process, particularly for families because the Privacy Rule would require a signed authorization from each family member or the family member’s personal representative. Whether an employee-applicant is the personal representative empowered by applicable state or other law to sign an authorization on behalf of a spouse or emancipated minor may prove problematic at best.

A third solution is for the health insurer to elect to become a hybrid entity. It may do this by designating in writing as its healthcare components all of its operations that perform its covered functions—those activities that involve its provision of or payment for the cost of medical care. Only these healthcare components of the hybridized health insurer will be required to comply with the Privacy Rule. Consequently, only individually identifiable health information that is created or received by or on behalf of these healthcare components will be protected health information. That means the health insurer’s nonhealthcare components will be outside the Privacy Rule, and individually identifiable health information created or received by those nonhealthcare components will not be protected health information.

95 See id. § 164.508(c)(1)(vi).
96 See supra note 29 for information regarding personal representative status under the Privacy Rule.
98 See id. § 164.105(a)(1)
99 See id. § 164.105(a)(2)(i)(C).
100 See id. § 164.105(a)(2)(i)(C).
To address the joint application dilemma, then, a health insurer may become a hybrid entity and leave its application intake and processing functions outside its healthcare components. Data intake and processing are not covered functions and, consequently, not mandated to be included as healthcare components. Data intake and processing are, at best, Business Associate-like activities, but the Privacy Rule does not compel a Covered Entity to include operations that perform Business Associate-like activities as healthcare components. Accordingly, by leaving its data intake and processing operations outside its healthcare components, a health insurer may receive and process joint applications in those noncovered operations. A health insurer therefore would be able to distribute the applications’ individually identifiable information to the life and disability issuer and to the insurer’s healthcare components. Only the individually identifiable health information received by the healthcare components will, in the hands of the healthcare components, be protected health information subject to the Privacy Rule.

V. Confidential Communications and Family Coverage EOBs

The Privacy Rule allows a health plan to send its explanations of benefits (EOBs) to its subscribers as a payment activity, even though the EOBs may contain protected health information of a spouse, emancipated minor, or other family member. Indeed, Department of Labor claim-procedure regulations require group health plans subject to the Employee Retirement Income Security Act of 1974 (ERISA) to give meaningful explanations of a denial of benefits on EOBs. Moreover, as the subscriber pays the premiums (at least the employee’s contribution), the subscriber has a legitimate interest in receiving information regarding claims payment under the insurance or benefit plan in which the subscriber and the subscriber’s family members participate.

The Privacy Rule requires a health plan to accommodate an enrollee’s reasonable request that protected health information be

101 See id. § 164.105(a)(2)(iii)(C).
102 See id. § 160.103 (stating business associate functions include “data analysis, processing or administration”).
103 See id. § 164.105(a)(2)(iii)(C).
104 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,607.
communicated in confidence to avoid endangering the enrollee.\textsuperscript{106} Hence, if a family member other than the subscriber demands that a health plan send EOBs relating to that member by alternative means (e.g., e-mail to an office or college computer) or to an alternative location (e.g., an office or college address) on claim of endangerment, the health plan must comply and not send those EOBs to the subscriber.

EOBs for claims paid for other family members, however, will show change in the family deductible caused by any claim paid on behalf of the family member who is receiving confidential communication. The health plan faces the dilemma that supplying a subscriber an EOB showing a change in family deductible after receipt of a confidential communication request is likely to convey to the subscriber, whom at least one family member may believe is dangerous, that one or more family members received healthcare. The dilemma is compounded if the subscriber contacts the health plan for an explanation for the change in family deductible.

There is no good solution to this quandary. An approach to soften the situation is to inform all enrollees in the health plan’s privacy practices notice that, notwithstanding their right to have confidential communications, EOBs and other information that the health plan issues to its subscribers about healthcare for which no confidential communication was requested may contain sufficient information to suggest to the subscriber that family members received healthcare for which confidential communication was requested. That at least will alert enrollees that confidential communication requests will not necessarily prevent a subscriber from learning of healthcare that is subject to such requests.

Another approach is to warn enrollees requesting confidential communications that, unless the enrollee personally pays for the healthcare for which confidential communications are requested, EOBs sent to the subscriber will reflect the health plan’s payment for that healthcare by the change in family deductible. This change in family deductible may convey to the subscriber that the family member received the healthcare that the member apparently wants to keep confidential.

\textsuperscript{106} 45 C.F.R. § 164.522(b)(1)(ii).
VI. Access Denial for Endangerment

The Privacy Rule allows a Covered Entity to withhold protected health information from an individual (or a personal representative) exercising the right of access if a healthcare professional determines that furnishing the information may endanger the individual or others.\textsuperscript{107} The Privacy Rule requires the Covered Entity to give the individual (or personal representative) a written explanation of the reason for denying access and the right to have the decision reviewed by another healthcare professional.\textsuperscript{108}

The Privacy Rule does not explain how to avoid endangering the individual or others when the Covered Entity is required to explain that it is withholding information to avoid endangering the individual or others. Covered Entities thus face the dilemma that they must state that information will not be supplied because it may endanger the individual or others, notwithstanding that such a statement may motivate the individual to untoward action to learn the information that a healthcare professional deems sufficiently dangerous to be kept from the individual. Put differently, the explanation mandated by the Privacy Rule may cause the very harm that withholding the protected health information is meant to avoid.

A Covered Entity should carefully craft the written explanation to minimize the potentially negative ramifications of this compliance conundrum. Simply stating that a healthcare professional has determined that certain medical information will not be disclosed to protect safety is probably sufficient for Privacy Rule compliance, though probably not sufficient to escape irritating, or worse, the individual who is given this explanation. On the other hand, turning over the dangerous medical information to the individual (an approach that the Privacy Rule does not prevent) could expose the Covered Entity to liability if the information does indeed cause the dangerous effect that a reviewing healthcare professional would predict. This is one “no-win” situation established by the Privacy Rule which a Covered Entity needs to manage with care, prudence, and hope.

\textsuperscript{107} Id. § 164.524(a)(3).
\textsuperscript{108} Id. § 164.524(d)(2).
VII. Conclusion

The Privacy Rule presents many compliance predicaments; this Article has examined and proposed solutions for several particularly troublesome ones. As operational experience with the Privacy Rule matures, DHHS undertakes enforcement, and the courts get opportunities to interpret the Privacy Rule, the soundness of these solutions may be verified or undermined, and other, perhaps better, solutions may emerge for these and for other compliance dilemmas.

For now, the prudent Covered Entity should try to address the dilemmas it faces with compliance strategies that reflect a reasonable balance between, on the one hand, its operational needs and sensible risk management and, on the other, the protective purposes of the Privacy Rule. The prudent Covered Entity will document these compliance strategies in the written policies and procedures required by the Privacy Rule, and will document its adherence with them to evidence that its practices conform to Privacy Rule obligations. Otherwise, a Covered Entity may face the enforcement predicament that “if it’s not documented, it didn’t happen.”

109 See id. § 164.530(i).
110 See id.