RAMSEYSOLUTIONS

Note: This statement is being provided to you because you have indicated that you use or wish to use RS Fax® for the purpose of sending and/or receiving faxes that may include "protected health information" under HIPAA/HITECH, and not for the purpose of storing any such faxes. Use of other Ramsey Solutions services or the use of RS Fax® to store such faxes may raise additional concerns, and must be addressed separately. This statement applies only to customers who are "covered entities" and/or "business associates" under HIPAA, as those terms are defined therein. If you are not such an entity, then this statement does not apply to you.

The purpose of this statement is to explain (i) Ramsey Solutions status under HIPAA[1] and the HITECH Act[2] in providing fax transmission services to you and, (ii) that HIPAA does not require you to enter into a "business associate agreement" ("BAA") with Ramsey Solutions in order to use these services.[3] By way of summary, HIPAA's Privacy and Security Rules ("Final Rules"), which are attached hereto as Exhibit A (see highlighted text), make clear that in providing transmission services – that is, services that allow you to send and receive faxes – Ramsey is not performing any services that would render it a "business associate" under HIPAA. This is because the Final Rules specifically provide that "data transmission organizations" like Ramsey Solutions that "do not require access to protected health information on a routine basis" are "not [to] be treated as business associates" because they are acting as "mere conduits" with respect to the "protected health information" ("PHI") at issue. As such, HIPAA does not require you to enter into a BAA with Ramsey Solutions, and you are free to avail yourself of the RS Fax® service without having such an agreement in place.

The Limited Scope of HIPAA's BAA Requirement

HIPAA does not require a "covered entity" and/or "business associate" to enter into a BAA with each and every vendor that might receive PHI. Rather, HIPAA's BAA requirement applies only where the vendor, by virtue of the services that it is providing, qualifies as the "business associate" of a "covered entity" or a "subcontractor" of a "business associate," which effectively puts the "subcontractor" on equal footing with a "business associate." If the vendor does not so qualify, then HIPAA does not require the "covered entity" to enter into a BAA with that vendor.

Ramsey Solutions Status Under HIPAA

The Final Rules make clear that the RS Fax® service provided by Ramsey Solutions is not one that requires "covered entities" or "business associates" to enter into a BAA with Ramsey Solutions. The Final Rules clarify that "data transmission organizations" like Ramsey Solutions that "do not require access to [PHI] on a routine basis" are "not [to] be treated as business associates." As the Final Rules explain, this clarification is consistent with the Department of Health and Human Services' longstanding interpretation of the definition of "business associate" as excluding "entities that act as mere conduits for the transport of [PHI] but do not access the information other than on a random or infrequent basis." Specifically, the Final Rules provide

that such conduit services, which expressly include electronic courier services, do not entail "'access on a routine basis' to [PHI]," which comprises a necessary condition for "business associate" status. Furthermore, to the extent that Ramsey Solutions must occasionally access faxes transmitted by you over Ramsey Solutions' network (e.g., as part of an effort to verify that our customers' faxes are arriving at their intended destinations), the Final Rules are clear that such "occasional, random access" falls short of the requisite "routine" access. Thus, the Final Rules conclusively establish that Ramsey Solutions is not acting as your "business associate" in providing fax transmission services to you.

1 The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
2 The Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009.
3 The purpose of this statement is purely informational. This statement is provided as part of Ramsey Solutions business negotiations with you and neither constitutes nor should be viewed or relied on as legal advice by you or anyone else. Neither Ramsey Solutions nor its attorneys are acting as your attorney.

In Light of Ramsey Solutions' Status, a BAA is Not Required

Because Ramsey Solutions is not acting as your "business associate" in providing fax transmission services to you, HIPAA imposes no obligation on you (or Ramsey Solutions) to enter into a BAA.

EXHIBIT A

FEDERAL REGISTER

Vol. 78 Friday,

No. 17 January 25, 2013

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 and 164

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945–AA03

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

AGENCY: Office for Civil Rights, Department of Health and Human Services.

ACTION: Final rule.

SUMMARY: The Department of Health and Human Services (HHS or ''the Department'') is issuing this final rule to: Modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement statutory amendments under the Health Information Technology for Economic and Clinical Health Act (''the HITECH Act'' or ''the Act'') to strengthen the privacy and security protection for individuals' health information; modify the rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) under the HITECH Act to address public comment received on the interim final rule; modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA); and make certain other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities.

DATES: *Effective date:* This final rule is effective on March 26, 2013.

Compliance date: Covered entities and business associates must comply with the applicable requirements of this final rule by September 23, 2013.

FOR FURTHER INFORMATION CONTACT: Andra Wicks 202–205–2292.

SUPPLEMENTARY INFORMATION:

I. Executive Summary and Background

A. Executive Summary

i. Purpose of the Regulatory Action

Need for the Regulatory Action

This final rule is needed to strengthen the privacy and security protections established under the Health Insurance Portability and Accountability of 1996 Act (HIPAA) for individual's health information maintained in electronic health records and other formats. This final rule also makes changes to the HIPAA rules that are designed to increase flexibility for and decrease burden on the regulated entities, as well as to harmonize certain requirements with those under the Department's Human Subjects Protections regulations. These changes are consistent with, and arise in part from, the Department's obligations under Executive Order 13563 to conduct a retrospective review of our existing regulations for the purpose of identifying ways to reduce costs and increase flexibilities under the HIPAA Rules. We discuss our specific burden reduction efforts more fully in the Regulatory Impact Analysis.

This final rule is comprised of four final rules, which have been combined to reduce the impact and number of times certain compliance activities need to be undertaken by the regulated entities.

Legal Authority for the Regulatory Action

The final rule implements changes to the HIPAA Rules under a number of authorities. First, the final rule modifies the Privacy, Security, and Enforcement Rules to strengthen privacy and security protections for health information and to improve enforcement as provided for by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The rule also includes final modifications to the Breach Notification Rule, which will replace an interim final rule originally published in 2009 as required by the HITECH Act. Second, the final rule revises the HIPAA Privacy Rule to increase privacy protections for genetic information as required by the Genetic Information Nondiscrimination Act of 2008 (GINA). Finally, the Department uses its general authority under HIPAA to make a number of changes to the Rules that are intended to increase workability and flexibility, decrease burden, and better harmonize the requirements with those under other Departmental regulations.

ii. Summary of Major Provisions

This omnibus final rule is comprised of the following four final rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:

- Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.
- Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
- Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
- Require modifications to, and redistribution of, a covered entity's notice of privacy practices.
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule (referenced immediately below), such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's ''harm'' threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.

4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

the regulation for one or more provisions. For purposes of this rule, the 180-day compliance period would not govern the time period required to modify those business associate agreements that qualify for the longer transition period in § 164.532, as we discuss further below.

Finally, the provisions of section 13402(j) of the HITECH Act apply to breaches of unsecured protected health information discovered on or after September 23, 2009, the date of the publication of the interim final rule. Thus, during the 180 day period before compliance with this final rule is required, covered entities and business associates are still required to comply with the breach notification requirements under the HITECH Act and must continue to comply with the requirements of the interim final rule. We believe that this transition period provides covered entities and business associates with adequate time to come into compliance with the revisions in this final rule and at the same time to continue to fulfill their breach notification obligations under the HITECH Act.

IV. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the HITECH Act; Other Modifications to the HIPAA Rules

The discussion below provides a section-by-section description of the final rule, as well as responds to public comments where substantive comments were received regarding particular provisions.

A. Subparts A and B of Part 160: Statutory Basis and Purpose, Applicability, Definitions, and Preemption of State Law

Subpart A of Part 160 of the HIPAA Rules contains general provisions that apply to all of the HIPAA Rules. Subpart B of Part 160 contains the regulatory provisions implementing HIPAA's preemption provisions. We proposed to amend a number of these provisions. Some of the proposed, and now final, changes are necessitated by the statutory changes made by the HITECH Act and GINA, while others are of a technical or conforming nature.

1. Subpart A—General Provisions, Section 160.101—Statutory Basis and Purpose

This section sets out the statutory basis and purpose of the HIPAA Rules. We proposed and include in this final rule a technical change to include references to the provisions of GINA and the HITECH Act upon which most of the regulatory changes below are based.

2. Subpart A—General Provisions, Section 160.102—Applicability

This section sets out to whom the HIPAA Rules apply. We proposed to add and include in this final rule a new paragraph (b) to make clear, consistent with the HITECH Act, that certain of the standards, requirements, and implementation specifications of the subchapter apply to business associates.

3. Subpart A—General Provisions, Section 160.103—Definitions

Section 160.103 contains definitions of terms that appear throughout the HIPAA Rules. The final rule modifies a number of these definitions to implement the HITECH Act and make other needed changes.

a. Definition of ''Business Associate''

The HIPAA Privacy and Security Rules permit a covered entity to disclose protected health information to a business associate, and allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, provided the covered entity obtains satisfactory assurances in the form of a contract or other arrangement that the business associate will appropriately safeguard the information. The HIPAA Rules define ''business associate'' generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. We proposed a number of modifications to the definition of ''business associate'' to implement the HITECH Act, to conform the term to the statutory provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b–21, et seq., and to make other changes to the definition.

i. Inclusion of Patient Safety Organizations

Proposed Rule

We proposed to add patient safety activities to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship. PSQIA, at 42 U.S.C. 299b–22(i)(1), provides that Patient Safety Organizations (PSOs) must be treated as business associates when applying the Privacy Rule. PSQIA provides for the establishment of PSOs to receive reports of patient safety events or concerns from providers and provide analyses of events to reporting providers. A reporting provider may be a HIPAA covered entity and, thus, information reported to a PSO may include protected health information that the PSO may analyze on behalf of the covered provider. The analysis of such information is a patient safety activity for purposes of PSQIA and the Patient Safety Rule, 42 CFR 3.10, et seq. While the HIPAA Rules as written would treat a PSO as a business associate when the PSO was performing quality analyses and other activities on behalf of a covered health care provider, we proposed this change to the definition of ''business associate'' to more clearly align the HIPAA and Patient Safety Rules.

Overview of Public Comment

Commenters on this topic supported the express inclusion of patient safety activities within the definition of ''business associate.''

Final Rule

The final rule adopts the proposed modification.

ii. Inclusion of Health Information Organizations (HIO), E-Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as Well as Vendors of Personal Health Records

Proposed Rule

Section 13408 of the HITECH Act provides that an organization, such as a Health Information Exchange Organization, E-prescribing Gateway, or Regional Health Information Organization, that provides data transmission of protected health information to a covered entity (or its business associate) and that requires access on a routine basis to such protected health information must be treated as a business associate for purposes of the Act and the HIPAA Privacy and Security Rules. Section 13408 also provides that a vendor that contracts with a covered entity to allow the covered entity to offer a personal health record to patients as part of the covered entity's electronic health record shall be treated as a business associate. Section 13408 requires that such organizations and vendors enter into a written business associate contract or other arrangement with the covered entity in accordance with the HIPAA Rules.

In accordance with the Act, we proposed to modify the definition of ''business associate'' to explicitly designate these persons as business associates. Specifically, we proposed to include in the definition: (1) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect

to protected health information to a covered entity and that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity.

We proposed to refer to ''Health Information Organization'' in the NPRM rather than ''Health Information Exchange Organization'' as used in the Act because it is our understanding that ''Health Information Organization'' is the more widely recognized and accepted term to describe an organization that oversees and governs the exchange of health-related information among organizations.[2] The Act also specifically refers to Regional Health Information Organizations; however, we did not believe the inclusion of the term in the definition of ''business associate'' was necessary as a Regional Health Information Organization is simply a Health Information Organization that governs health information exchange among organizations within a defined geographic area.[3] Further, the specific terms of ''Health Information Organization'' and ''E-prescribing Gateway'' were included as merely illustrative of the types of organizations that would fall within this paragraph of the definition of ''business associate.'' We requested comment on the use of these terms within the definition and whether additional clarifications or additions were necessary.

Section 13408 also provides that the data transmission organizations that the Act requires to be treated as business associates are those that require access to protected health information on a routine basis. Conversely, data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates. This is consistent with our prior interpretation of the definition of ''business associate,'' through which we have stated that entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis are not business associates. See *http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html.* In contrast, entities that manage the exchange of protected health information through a network, including providing record locator services and performing various oversight and governance functions for electronic health information exchange, have more than ''random'' access to protected health information and thus, would fall within the definition of ''business associate.''

Overview of Public Comments

Commenters generally supported the inclusion of Health Information Organizations, personal health record vendors, and similar entities in the definition of ''business associate.'' However, commenters sought various clarifications as discussed below.

Commenters generally supported use of the term Health Information Organization in lieu of more restrictive terms, such as Regional Health Information Organization. Some commenters suggested that the term Health Information Organization be defined, so as to avoid confusion as the industry develops, and suggested various alternatives for doing so. Several commenters recommended that the Office for Civil Rights (OCR) maintain a Web site link that lists current terms for entities that OCR considers to be Health Information Organizations.

Other commenters requested clarification on what it means to have ''access on a routine basis'' to protected health information for purposes of the definition and determining whether certain entities are excluded as mere conduits. For example, commenters asked whether the definition of business associate would include broadband suppliers or internet service providers, vendors that only have the potential to come into contact with protected health information, or entities contracted on a contingency basis that may at some point in the future have access to protected health information. Several document storage companies argued that entities like theirs should be characterized as conduits, as they do not view the protected health information they store.

Several commenters sought clarification regarding when personal health record vendors would be considered business associates. For example, commenters asked whether personal health record vendors would be business associates when the vendor provided the personal health record in collaboration with the covered entity, when the personal health record is linked to a covered entity's electronic health record, or when the personal health record is offered independently to the individual, among other scenarios. One commenter suggested that a vendor offering a personal health record to a patient on behalf of a covered entity only acts as a conduit because there is no access by the vendor to protected health information; another commenter suggested that personal health record vendors be business associates only when they have routine access to protected health information.

Final Rule

The final rule adopts the language that expressly designates as business associates: (1) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity.

We decline to provide a definition for Health Information Organization. We recognize that the industry continues to develop and thus the type of entities that may be considered Health Information Organizations continues to evolve. For this reason, we do not think it prudent to include in the regulation a specific definition at this time. We anticipate continuing to issue guidance in the future on our web site on the types of entities that do and do not fall within the definition of business associate, which can be updated as the industry evolves.

Regarding what it means to have ''access on a routine basis'' to protected health information with respect to determining which types of data transmission services are business associates versus mere conduits, such a determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to protected health information to perform the service for the covered entity. The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to protected health information when it reviews whether the data transmitted over its network is arriving

[2] Department of Health and Human Services Office of the National Coordinator for Health Information Technology, The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology: Defining Key Health Information Terms, Pg. 24 (2008).

[3] *Id.* at 25.

at its intended destination. Such occasional, random access to protected health information would not qualify the company as a business associate. In contrast, an entity that requires access to protected health information in order to perform a service for a covered entity, such as a Health Information Organization that manages the exchange of protected health information through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate. We intend to issue further guidance in this area as electronic health information exchange continues to evolve.

We note that the conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission. In contrast, an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information. We recognize that in both situations, the entity providing the service to the covered entity has the opportunity to access the protected health information. However, the difference between the two situations is the transient versus persistent nature of that opportunity. For example, a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of ''business associate'' to generally provide that a business associate includes a person who ''creates, receives, *maintains,* or transmits'' (emphasis added) protected health information on behalf of a covered entity.

Several commenters sought clarification on when a personal health record vendor would be providing a personal health record ''on behalf of'' a covered entity and thus, would be a business associate for purposes of the HIPAA Rules. As with data transmission services, determining whether a personal health record vendor is a business associate is a fact specific determination. A personal health record vendor is not a business associate of a covered entity solely by virtue of entering into an interoperability relationship with a covered entity. For example, when a personal health record vendor and a covered entity establish the electronic means for a covered entity's electronic health record to send protected health information to the personal health record vendor pursuant to the individual's written authorization, it does not mean that the personal health record vendor is offering the personal health record on behalf of the covered entity, even if there is an agreement between the personal health record vendor and the covered entity governing the exchange of data (such as an agreement specifying the technical specifications for exchanging of data or specifying that such data shall be kept confidential). In contrast, when a covered entity hires a vendor to provide and manage a personal health record service the covered entity wishes to offer its patients or enrollees, and provides the vendor with access to protected health information in order to do so, the personal health record vendor is a business associate.

A personal health record vendor may offer personal health records directly to individuals and may also offer personal health records on behalf of covered entities. In such cases, the personal health record vendor is only subject to HIPAA as a business associate with respect to personal health records that are offered to individuals on behalf of covered entities.

We also clarify that, contrary to one commenter's suggestion, a personal health record vendor that offers a personal health record to a patient on behalf of a covered entity does not act merely as a conduit. Rather, the personal health record vendor is maintaining protected health information on behalf of the covered entity (for the benefit of the individual). Further, a personal health record vendor that operates a personal health record on behalf of a covered entity is a business associate if it has access to protected health information, regardless of whether the personal health record vendor actually exercises this access. We believe the revisions to the definition of ''business associate'' discussed above clarify these points. As with other aspects of the definition of ''business associate,'' we intend to provide future guidance on when a personal health record vendor is a business associate for purposes of the HIPAA Rules.

Response to Other Public Comments

Comment: One commenter recommended that the term ''person'' used in describing who provides transmission services to a covered entity be clarified to apply also to entities and organizations.

Response: The term ''person'' as defined at § 160.103 includes entities as well as natural persons.

Comment: One commenter asked whether subcontractors that support business associates with personal health record related functions are subject to the breach notification requirements under the HIPAA Breach Notification Rule or that of the FTC.

Response: As discussed below, a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate, including with respect to personal health record functions, is a HIPAA business associate and thus, is subject to the HIPAA Breach Notification Rule and not that of the FTC. The analysis of whether a subcontractor is acting on behalf of a business associate is the same analysis as discussed above with respect to whether a business associate is acting on behalf of a covered entity.

iii. Inclusion of Subcontractors

Proposed Rule

We proposed in the definition of ''business associate'' to provide that subcontractors of a covered entity, i.e., those persons that perform functions for or provide services to a business associate other than in the capacity as a member of the business associate's workforce, are also business associates to the extent that they require access to protected health information. We also proposed to define ''subcontractor'' in § 160.103 as a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate. Even though we used the term ''subcontractor,'' which implies there is a contract in place between the parties, the definition would apply to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate contract with the person. We requested comment on the use of the term ''subcontractor'' and its proposed definition.

The intent of the proposed extension of the Rules to subcontractors was to avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity