June 2001

HIPAA Becomes Reality: Compliance with New Privacy, Security, and Electronic Transmission Standards

Mary Beth Johnson
*Womble Carlyle Sandridge & Rice, PLLC*

Leighton Roper
*Womble Carlyle Sandridge & Rice, PLLC*

Follow this and additional works at: https://researchrepository.wvu.edu/wvlr

Part of the Health Law and Policy Commons, Internet Law Commons, and the Privacy Law Commons

**Recommended Citation**


Available at: https://researchrepository.wvu.edu/wvlr/vol103/iss4/7

This Article is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact researchrepository@mail.wvu.edu.
HIPAA BECOMES REALITY:  
COMPLIANCE WITH NEW PRIVACY, SECURITY, 
AND ELECTRONIC TRANSMISSION STANDARDS

Mary Beth Johnston*  
Leighton Roper**

I. INTRODUCTION ................................................................. 542

II. PRIVACY AND SECURITY PROVISIONS .................................... 546  
A. Proposed Security Rules ...................................................... 546  
B. Proposed Privacy Rules ....................................................... 549  
C. Criticism of the Proposed Privacy and Security Rules .............. 552  
D. Final Privacy Rules ............................................................. 554  
1. New/Modified Definitions .................................................... 554  
2. Rule of Nondisclosure; “Permission”  
   Requirements/Exceptions; Additional  
   Limitations ............................................................................. 556  
3. Required Notice Accompanying Individual  
   Permission ............................................................................ 559  
4. Expanded Rules Governing Uses and  
   Disclosures in Complex Business  
   Associations: Organized Health Care  
   Arrangements, Affiliated Entities, Multiple  
   Covered Function Entities, Component  
   Entities, and Group Health Plans .................................... 560  
5. Business Associate Rules ....................................................... 562  
6. Individual Rights ................................................................. 565  
7. Overall Compliance with the Final Rule;  
   Required Administrative Procedures ..................................... 566

III. ELECTRONIC TRANSACTION AND CODE SET STANDARDS ........ 568  
A. Statutory Background ........................................................... 568  
B. Final Electronic Transaction and Code Set Rules ...................... 569

IV. CONCLUSION ........................................................................... 572

* Ms. Johnston is a Partner and Health Law Section Chair of Womble Carlyle Sandridge & Rice,  
   PLLC in Research Triangle Park, North Carolina. JD 1983, Campbell University School of Law; AB 1980,  
   University of North Carolina—Chapel Hill. Ms. Johnston is the past president of the North Carolina Society  
   of Health Care Attorneys, is the Vice-chair of the American Bar Association Health Law Section’s eHealth  
   and Privacy Interest Group, and has made numerous professional presentations about compliance with the  
   new HIPAA regulations discussed in this article.

** Mr. Roper is an associate in the Research Triangle Park, North Carolina, office of Womble Carlyle  
   Sandridge & Rice, PLLC. JD 1999, Duke University; BA 1990, University of Virginia. Mr. Roper was the  
   president of the Duke Health Law Society, and is a member of the American Health Lawyers Association and  
   the North Carolina Society of Health Care Attorneys.
I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") enacted by Congress contained five health care-related titles. The scope of the law was enormously broad, ranging from requiring the portability of health insurance to authorizing the imposition of the stronger health care fraud sanctions. Title II, Subtitle F of HIPAA, known as the “administrative simplification provisions,” was intended “to improve the Medicare . . . [and] Medicaid program . . . , and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.” Further, the provisions required that the federal Department of Health and Human Services (“DHHS”) adopt standards that are consistent with the objective of reducing administrative costs of providing and paying for health care.

The administrative simplification provisions received very little attention until 1998, when DHHS began releasing long-delayed regulations. DHHS has since issued proposed security, and final privacy and electronic transaction/code set requirements and standards. The privacy and electronic transaction/code set rules take effect February 26, 2003 and October 16, 2002, respectively (except for small health plans, which will have an additional year to comply). All standards and requirements apply, unless otherwise specified, to “covered entities” - health


2 42 U.S.C. § 1320d note (2000). HIPAA provides that standards (and modifications to such standards) are to be developed by “standard-setting organizations,” including the National Council for Prescription Drug Programs, the National Uniform Billing Committee, the National Uniform Claim Committee, the Workgroup for Electronic Data Exchange, and the American Dental Association; however, DHHS may adopt different standards to the extent that they are “consistent with the objective of reducing administrative costs of providing and paying for health care.” Id. §§ 1320d(8), d-1(b), (c). Standards may not require disclosure of trade secrets or other confidential information. See id. § 1320d-1(e). The National Committee on Vital and Health Statistics is to make recommendations to DHHS regarding compliance with the standards. See id. § 1320d-1(f).

3 See id. § 1320d-1(0)(2)(A)(0), d-3(a); see also infra section II(B) for a discussion of the genesis of DHHS’s privacy rulemaking authority. Note that under the statute, DHHS generally may not require that covered entities disclose trade secrets or other confidential information. See 42 U.S.C. § 1320d-1(0).


7 See Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50,312 (2000) (to be codified at 45 C.F.R. pt. 160, 162). This article does not address several other rules promulgated (or to be promulgated) under HIPAA, including rules addressing electronic signatures; “unique identifiers” for health care providers, employers and individuals; claims attachments; and enforcement. DHHS’s online schedule for developing and finalizing these rules may be found online at <http://aspe.os.dhhs.gov/admsimp/pubsched.htm>.

8 HIPAA specifically exempts the processing of payment transactions by or for financial institutions (as defined in 12 U.S.C. § 3401), as well as (1) entities “engaged in activities of a financial institution” or (2)
plans, health care clearinghouses, and health care providers - that transmit or maintain any health information via electronic media in connection with a covered transaction. Covered transactions include most financial and administrative transactions, such as health claims or equivalent encounter information, health claims attachments, enrollment and disenrollment in a health plan, eligibility for a health plan, health care payment and remittance advice, health plan premium payments, first report of injury, health claim status, and referral certification and authorization.

entities engaging in certain activities “for a financial institution.” 42 U.S.C. § 1320d-8 (2000). We discuss additional regulatory exceptions in connection with our analysis of specific rules, infra parts II and III.

42 U.S.C. § 1320d(5) defines a “health plan” as “an individual or group plan that provides, or pays the cost of medical care . . . .” Health plans include, but are not limited to Medicare, Medicare supplemental, Medicare + Choice, and Medicaid plans; SCHIP plans; state high risk pools; group health plans with 50 or more participants (except employer-sponsored plans); HMOs; health insurers (except group health plans); long-term care policies; employee welfare benefit plans or like organizations; military and veterans health plans; CHAMPUS plans; Indian health service plans; and FEHBP plans. See 45 C.F.R. § 160.103 (2001).

42 U.S.C. § 1320d(2) defines a “health care clearinghouse” as “a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.” Regulations provide a clearer definition: “Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and value-added networks and switches, that does either of the following functions: (1) [p]rocesses or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) [r]eceives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.” 45 C.F.R. § 160.103. See also 42 U.S.C. § 1320d-4(a)(2)(B), -4(b)(3) (allowing covered entities to achieve HIPAA compliance by submitting or receiving information via a health care clearinghouse).

42 U.S.C. § 1320d(3) defines a “health care provider” as “a provider of services . . . . medical or other health services . . . . and any other person furnishing health care services or supplies.” Regulations provide: “Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.” 45 C.F.R. § 160.103 (2001).

“Health information” is “information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (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.” 42 U.S.C. § 1320d(4); 45 C.F.R. § 160.103(2001).

“Electronic media means the mode of electronic transmission. It includes the Internet (wide-open), Extranet . . . , leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.” 65 C.F.R. § 162.103 (2001).

See id. (defining “covered entity”).

See Adele A. Waller, Preparing for the Complexities of Administrative Simplification Under HIPAA, in HEALTH L. HANDBOOK at 678 (West 1999).

HIPAA's penalty provisions provide the basis for the enforcement of the requirements and standards (a final compliance and enforcement rule is forthcoming). Each failure to comply is punishable by a fine of up to $100, not to exceed $25,000 in a calendar year for violations of the same requirement or prohibition. However, violations may not be punished if they are (1) not known and could not have been discovered through the exercise of reasonable diligence or (2) due to a reasonable cause not willful neglect and are cured within 30 days. Additionally, DHHS may waive penalties for reasonable, non-willful violations to the extent that they are found to be "excessive."

In addition to penalizing non-compliance with HIPAA's requirements and standards, HIPAA separately punishes any person who "knowingly" obtains or discloses "individually identifiable health information." Individually identifiable health information (hereinafter referred to as "protected information") includes "[a]ny information, including demographic information collected from an individual,"

(A) that 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—

Reg. 82,480 (2000).

See 42 U.S.C. §§ 1320d-5 to 6 (establishing exclusive penalties for (1) failure to comply with regulatory requirements and standards and (2) wrongful disclosure of individually identifiable health information).

DHHS plans to issue compliance and enforcement regulations prior to the first effective date for HIPAA rules, October 16, 2002. 65 Fed. Reg. 50,343 (2000) ("We plan to publish an NPRM requesting public comments next year, and to subsequently issue a final compliance and enforcement regulation that will become effective prior to the first compliance dates of these rules."). Under current rules (last amended in the final privacy rule, discussed infra part II.D), DHHS may seek entities' cooperation in ensuring compliance with the rule, and DHHS may offer technical compliance assistance. 45 C.F.R § 160.304 (2001). Any person (not just an individual) may file a privacy complaint with DHHS within 180 days of the time that the complainant knew or should have known of the violation (unless the Secretary waives statute of limitation for good cause shown). See id. § 160.306. A complaint may trigger investigation. See id. Additionally, DHHS may conduct compliance reviews; in addition to providing DHHS with ordinary records access during normal business hours, covered entities must give DHHS access at any time without notice where exigent circumstances exist, such as where documents may be hidden or destroyed. See id. 160.308-312.


See id. § 1320d-5(b).

See id. § 1320d-5(b)(4).

See id. § 1320d-6(a).
HIPAA BECOMES REALITY

(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.23

Offenders shall be (1) fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.24

Due to its (increasing) breadth, HIPAA promises to dramatically change the health care industry’s use of technology and individual health care data, requiring industry participants to dedicate significant resources to achieving compliance.25 However, many sectors of the health care industry remain unprepared for HIPAA.26 In an effort to provide a starting point for HIPAA compliance activities, this article summarizes the key provisions of privacy, security and electronic transaction rules. Readers are cautioned not to rely solely on this article for guidance, however, as analysis may vary according to the facts and circumstances surrounding a particular transaction or entity, new regulatory pronouncements, and the applicability of certain federal and state laws not addressed herein.27


25 In 1998, the Workgroup for Electronic Data Interchange (WEDI) estimated the cost of implementing HIPAA rules (excluding privacy rules) at between $5.3 - $17 billion. See Anthony Colletti, HIPAA: An Overview, ABA HEALTH LAWYER, Oct. 2000, at 16 & n1; 63 Fed. Reg. 60,006-07 (2000). The same year, DHHS projected the additional cost of compliance with HIPAA privacy standards to be “at least” $3.8 billion over five years. However, industry representatives have estimated compliance costs at up to ten times DHHS estimates. See id. As of December of last year, the hospital industry estimated the cost of compliance with all rules at $22.5 billion. See First Consulting Group (for the American Hospital Association), Impact of the Proposed Privacy Rule on the Hospital Industry, <http://www.aha.org/hipaa/resources/impactPrivacyDec2000.asp>.

26 Noncompliance with the security rule, for example, is well documented. See Thom Wilder, Noncompliance with HIPAA Security Proposal Common, Experts Say, AHLA E-HEALTH L. & POL’Y REP., Dec. 21, 2000. For instance, while a majority of payers reported having created HIPAA-compliance staff positions/committees and conducted required risk assessments, only 24% of hospitals have conducted an information security audit and only half of the remaining 76% expect to complete such an audit by next April. See Payers Outpace Providers in HIPAA Compliance, Study Says, AHLA E-HEALTH L. & POL’Y REP., Oct. 26, 2000; Survey: Hospitals Unprepared for HIPAA Security, INTERNET HEALTHCARE MAG., Nov. 15, 2000, <http://www.internethealthcaremag.com/html/news/NewsStory.cfm?DID=2065>. Additionally, 40% of hospitals had not selected an information security officer (a requirement under the proposed HIPAA security rule), 30% had not formed organizational committees to examine HIPAA issues, and only 5% said that they have an annual budget for HIPAA compliance. See id.

II. PRIVACY AND SECURITY PROVISIONS

A. Proposed Security Rules

HIPAA required DHHS to adopt health information security standards applicable to covered entities that maintain or transmit electronic health information. The security standards were intended to implement “reasonable and appropriate administrative, technical, and physical safeguards —

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated —

(i) threats or hazards to the security or integrity of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part . . . by the officers and employees of such person.”

The proposed electronic security rule, promulgated by DHHS on August 12, 1998, requires covered entities (including “intra-corporate” entities) to implement overlapping administrative safeguards, physical safeguards, technical
security services,\textsuperscript{31} and technical security mechanisms\textsuperscript{32} in order to safeguard electronically maintained or transmitted protected information.\textsuperscript{33} The safeguards formalize the security rules' overarching goals of forcing entities to conduct pre-implementation internal risk assessments, develop and implement appropriate organizational and technical security measures, and document the most current implementation of these measures through promulgation of appropriate policies and procedures.\textsuperscript{34} The proposed rules exempt (1) paper transactions and (2) acceptance by and transmission of certain nonstandard communications by health care clearinghouses.\textsuperscript{35}

One important feature of the security rules is that covered entities are allowed a high degree of flexibility in achieving compliance, permitting them to adopt methods and technologies that are appropriate to their particular needs (as

\begin{itemize}
\item employee sanction policies and a security policy; termination procedures including changing locks; removal from access lists; removal from user accounts; and collection of keys and other forms of access; and training including security awareness training; periodic security reminders; education regarding virus protection, the importance of monitoring and reporting login success and failure, and maintaining password confidentiality. See id.
\end{itemize}

\textsuperscript{30} See id. at 43,253-54. Required physical safeguards include: assignment of security responsibilities; media controls regarding the receipt and removal of hardware and software from the facility, including access control, accountability for tracing removed property, a data backup system, a data storage system and a data disposal system; physical access controls, including disaster data recovery plan, emergency mode operation plan, equipment control into and out of the facility, a facility security plan to prevent unauthorized physical access, procedures for verifying access authorization before granting physical access, documentation of maintenance to hardware and the facility, need to know procedures limiting access to only necessary data, visitor sign in procedures (if appropriate), and restriction of testing and revision to authorized personnel; policies on workstation use; creation of a secure workstation location; and security awareness training. See id.

\begin{itemize}
\item employee sanction policies and a security policy; termination procedures including changing locks; removal from access lists; removal from user accounts; and collection of keys and other forms of access; and training including security awareness training; periodic security reminders; education regarding virus protection, the importance of monitoring and reporting login success and failure, and maintaining password confidentiality. See id.
\end{itemize}

\textsuperscript{31} See id. at 43,253-54. Required technical security services include: access control, including a procedure for emergency access; either context-based access, role-based access, or user-based access; and the optional use of encryption; audit controls to examine system activity; authorization controls using either role-based or user-based access; data authentication; and entity authentication, including automatic logoff, a unique user identifier, and either biometric identification, password, personal identification number, telephone callback procedure, or token. See id.

\textsuperscript{32} See id. at 43,255. Required technical security mechanisms include: if the health care organization uses electronic communications or an electronic network, then integrity controls to insure the validity of data being transmitted or stored; message authentication to confirm the message received matches the message sent; either access controls or encryption; and, if the health care organization uses an electronic network, mechanisms also include an alarm system to detect abnormal system conditions; an audit trail for use in a security audit; entity identification to identify authorized and unauthorized users; and event reporting of irregularities in the physical elements of the system or the completion of a significant task. See id.


\textsuperscript{35} See 45 C.F.R. § 142.105; see also 63 Fed. Reg. at 43,245-46 (1998). Note that the proposed security rules also exempt "faxback" and "HTML interaction between a server and browser by which the data elements of a transaction are solicited from a user." However, these exemptions will likely be eliminated in the final security rules, given DHHS's revocation of an identical exemption in the final electronic transmission and code set rules, discussed infra part III.B.
identified through individual security risk analysis). However, covered entities must be aware that "more stringent" security measures may be applied either by federal or state agency rule, or by private agreement.

Covered entities can begin certain organizational compliance activities prior to issuance of the final rule. First, covered entities should arrange for a legal briefing on current security rules, as well as other applicable federal and state laws. Second, covered entities should appoint an information security officer, form a health information security committee, and begin planning for security certification. Third, covered entities should budget for, conduct and document an internal security risk analysis with an eye towards the proposed security and, as discussed below, the final privacy rules. Fourth, covered entities should ensure that HIPAA-mandated provisions are added to current and existing contracts governing purchases of new technology (including encryption software and other technology products such as new systems or clinical equipment) and relationships with vendors/customers having access to protected information. Fifth, once security needs have been assessed/documented and necessary contract changes have been implemented, covered entities can begin implementing administrative and physical safeguards (as needed) and training staff.

Achieving technical security compliance, though merely a means of supporting covered entities' policy and procedural decisions, may present a more substantial obstacle. Some commentators have questioned whether technical compliance is currently possible given an alleged dearth of either (1) easily-installed, inexpensive security software, or (2) vendors offering compliant systems capable of interfacing with those of any other covered entity. Particular attention has focused on the technical difficulties of using PKI (or "public key infrastructure"), a double-layered encryption system requiring implementation by

---

36 See 63 Fed. Reg. at 43,249-50 (1998); Waller, supra note 15, at 691; Alan Goldberg, HIPAA Myths and Realities, AHLA E-HEALTH L. & POL’Y REP., Oct. 12, 2000 (refuting myths that HIPAA mandates covered entities’ acquisition of certain technologies to achieve compliance); Jonathan P. Tomes, HIPAA’s Privacy and Security Regulations: Administrative Complication, Not Simplification, HEALTH L. DIG., Jan. 2000, at 13 (flexibility of standard derived from the regulatory definition of risk analysis at § 142.308(b)(10)(i)).


39 See articles listed supra note 38; see also Risk Studies Will Help Industry Prepare for Final Privacy Rules, E-HEALTH L. & POL’Y REP., Oct. 26, 2000. This step is not only required by the rules, but is also useful in creating awareness of internal privacy and security problems, thereby forcing management to focus on specific HIPAA issues.

40 See AFHECHT-WEDI, 1999 Healthcare Internet Security Interoperability Pilot, available online at <http://www.xmissioncom/~zubeldia/edisc/reportsfinalfinalreport.doc> (discussing a variety of current technical obstacles that prevent secure health care transactions over the Internet); see also Marks, supra note 38. A related concern is with “vaporware,” or technology that does not assist in accomplishing HIPAA purposes despite representations to the contrary. Id.
information senders and receivers, to solve thorny informational integrity, secure transmission and sender authentication issues. While there are currently no pat answers to these and other technical concerns, the complexities of solving technical security issues underscores the need for early action on security compliance.

B. Proposed Privacy Rules

Introduction. HIPAA required Congress to enact privacy standards by August 21, 1999; however, HIPAA also vested DHHS with rulemaking authority in the event of Congress' failure to meet its self-imposed deadline. Specifically, DHHS was required to promulgate, within 42 months of the date of Congress' failure to timely enact privacy legislation, final privacy rules that at minimum addressed

1. the rights that an individual who is a subject of individually identifiable health information should have;

2. the procedures that should be established for the exercise of such rights; and

3. the uses and disclosures of such information that should be authorized or required.

Congress unsurprisingly failed to meet its deadline. Thus, on November 3, 1999, DHHS promulgated proposed privacy rules governing uses and disclosure of electronically maintained and transmitted protected information.

The remainder of this subsection II(B) and the corresponding endnotes summarize the key provisions of the proposed rules. Note that some regulatory references in this section may have been superceded in the final rule, discussed infra in section II(D).

Rule of nondisclosure; business partners. Covered entities were
prohibited from disclosing protected health information, except where disclosure was: (1) the "minimum necessary" information needed to carry out "treatment, payment, or health care operations;" (2) "authorized" by the individual; (3) consistent with certain public policy purposes or for compliance purposes; or (4)

---

46 "Disclosure" meant "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information." Id. § 164.504.

47 When protected information was disclosed pursuant to the rule, a covered entity was to make all reasonable efforts not to disclose more than the minimum amount of information necessary to accomplish use's or disclosure's intended purpose. See id. § 164.506(b). Accordingly, in addition to adopting procedural "safeguards" against disclosure, covered entities were required to develop procedures to identify appropriate persons charged with determining what information should be used or disclosed, to ensure these persons made the minimum necessary determinations, and, within the technological capabilities, to ensure that such determinations were made on a case-by-case basis. Covered entities were permitted to rely, when making permitted-but-not-required disclosures to public entities that the information requested was the minimum necessary. Additionally, covered entities were to allow individuals "to request," subject to several exceptions, that uses or disclosures of protected health information be restricted. To comply with this standard, health care providers were to provide individuals with an opportunity to make the request, provide for documentation of the restrictions agreed to, provide for compliance with the request, and provide for notification of others to whom the information is disclosed of such restrictions. See id.

48 "Health care operations meant the following activities undertaken by or on behalf of a covered entity that is a health plan or health care provider for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment: (1) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines; (2) reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which undergraduate and graduate students and trainees in areas of health care learn under supervision to practice as health care providers, accreditation, certification, licensing or credentialing activities; (3) insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the individuals are already enrolled in the health plan conducting such activities and the use or disclosure of protected health information relates to an existing contract of insurance (including the renewal of such a contract); (4) conducting or arranging for medical review and auditing services, including fraud and abuse detection and compliance programs; and (5) compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding. 45 C.F.R. § 164.504.

49 Id. § 164.508 (2001). Generally, an authorization was required to use or disclose protected health information (1) when the individual requested disclosure (2) a covered entity requested disclosure for purposes other than treatment, payment, or health care operations, and (3) for disclosure of psychotherapy notes or obtaining research information unrelated to treatment. See id. § 164.508(a). Pre-disclosure authorization was also expressly required for (1) marketing health information; (2) disclosing the information by sale, rental, or barter; (3) using and disclosing the health information to a non-health related covered entity, e.g., for use in marketing life or casualty insurance or banking services; (4) disclosing, prior to an individual's enrollment in a health plan, the health information to a health plan or health care provider for making eligibility or enrollment determinations relating to the individual, or for underwriting or risk rating determinations; (5) disclosing the health information to an employer for employment determinations; and (6) using or disclosing the health information for fund-raising purposes. See id. § 164.508(a)(2)(ii). An authorization was deemed defective if: (1) the expiration date had passed or the form was not fully completed, (2) the health care organization knew the authorization has been revoked, (3) the form lacked a required element (specified in C.F.R. § 164.508(c-f)), or (4) the health care organization knew the information on the form was false. See id. § 164.508(b)(2)(i-iv). Note also that health care organizations were required to have procedures to request only the minimum amount of necessary information be used or disclosed and to provide the individual with a copy of the authorization. See id. § 164.508(b)(2)(i-iv).

50 Individual authorization was not required for "public" uses and disclosures set out at former 45 C.F.R. § 164.510 (2001); we do not list them here because many were retained as exceptions in the final rule, discussed infra. Covered entities were required to disclose protected health information to the individual or to DHHS to determine compliance with applicable standards. See id. § 164.522(d)(3).
of "de-identified" information. A covered entity could, subject to certain conditions, use or disclose information from "identifying" elements that were removed or otherwise concealed. See id. § 164.506(d)(1). Most elements were retained in an exception to the final rule, discussed infra.

52 The key features of the business partner relationship were that the business partner was performing an activity or function for or on behalf of the covered entity and that the business partner received protected health information from the covered entity as part of providing such activity or function. Business partners included contractors or other persons who received protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. They did not include persons who were members of the covered entity's workforce. 64 Fed. Reg. 59,947 (1999) (to be codified at 45 C.F.R. § 164.506).

53 See id. at 59,947-50.

54 Satisfactory assurances entailed the parties agreement to contractual provisions establishing permitted and required uses and disclosures of protected information, and providing that the partner would take specified actions to safeguard the confidentiality of information both internally and upon disclosure to subcontractors. These contractual provisions were substantially adopted in the final "business associate" rules, discussed infra section II(D)(5).

55 45 C.F.R. § 164.506(e)(1). Note that business partner agreements, applicable to entities performing activities "for or on behalf of" covered providers (64 Fed. Reg. at 59,947), may be less restrictive than the security regulations' "chain of trust" agreements, discussed supra. Chain of trust agreements apply to "every party to whom protected information is disclosed." However, requirements for business partner agreements are clearly more extensive. See Brittin, supra note 44, at 1951-52 (emphasis added).

56 A material breach - one that the health care organization knew or should have known about and for which it failed to take reasonable steps to cure or terminate the contract - constituted noncompliance with these rules. See 64 Fed. Reg. at 59,949-50.

57 See id. § 164.512.

58 See id. § 164.514.

59 See id. § 164.516.
Covered entities were required to take a number of administrative measures to implement the privacy rule, including posting a privacy policy; designating privacy officials and privacy complaint contact persons; establishing privacy procedures; educating staff on these policies and procedures; and establishing sanctions for privacy violations. Covered entities were further required to document their compliance with the privacy regulations for purposes of administrative review, submit compliance reports as deemed necessary by DHHS; cooperate with any DHHS review of privacy policies, procedures, and practices; permit DHHS access to pertinent information regarding its compliance, and refrain from intimidating or retaliatory acts against whistleblowers.

C. Criticism of the Proposed Privacy and Security Rules

Industry criticism of the proposed privacy and security rules followed four general themes, including the high cost of implementation, regulatory burdens, interactions between HIPAA and preexisting privacy laws, and other specific deficiencies.

High cost. Critics most often complained of the high cost of technological acquisitions required to achieve compliance (in conflict with HIPAA's cost-saving purpose); "draconian" penalties for noncompliance; increased potential for costly litigation; and the rules' negative impact on hospital fundraising.

60 See id. § 164.515.
61 See 45 C.F.R. § 164.518.
62 See id. § 164.520. Specified documentation must be maintained for six years.
63 See id. § 164.522.
64 See Tomes, supra note 36, at 17-18 (citing increased costs of honoring "individual rights" created by privacy rules, meeting increased accreditation requirements, and implementing of security measures, as well as the regulations' alleged disproportionate impact on small practices). Furthermore, many have argued that DHHS' cost estimates under the proposed rules were grossly understated. See AHA cost study, supra note 25; Government Underestimated HIPAA Privacy Cost, AHA Says, AH LA E-HEALTH L. & POL'Y REP., Dec. 21, 2000. A 1999 Blue Cross/Blue Shield survey estimated the overall cost of compliance with confidentiality provisions at $43 billion. See Nahra, Beyond HIPAA, supra note 27, at 1057 n.10.
65 See Tomes supra note 36, at 16 n.15 (arguing that penalties are as great as those imposed for Medicare and Medicaid fraud and abuse, with the same potential to increase over time). See also Nahra, Confusion Reigns Supreme, supra note 27, at 75.
66 See Anticipated Privacy Rule Raises Private Liability Concerns, E-HEALTH L. & POL'Y REP., Dec. 7, 2000; Anticipated Privacy Rule Could Give Tort Lawyers New Weapon, Some Say, Health L. Rep. (BNA) No. 48, at 1852 (Dec. 14, 2000); Federal Prosecutor Warns E-Health Attorneys to Counsel Clients on Web Privacy Protections, E-HEALTH LAW & POL'Y REP., Sep. 14, 2000. See Tomes, supra note 36, at 17 (arguing that the regulations could be adopted as the standard of care in state tort litigation; that regulations arguably create a private right of action for individuals to providers sue under contract theory as third party beneficiaries to business partner agreements; and that much litigation will center on federal pre-emption over the "stringency" of state law); see also Nahra, Beyond HIPAA, supra note 27.
67 See Proposed Privacy Rules Put Nonprofits Fund-raising at Risk, E-HEALTH LAW & POL'Y REP.,
Regulatory burden. 68 One commentator specifically noted the standards’ unprecedented breadth of coverage. 69 Others, while contending that DHHS had exceeded its statutory authority by regulating the privacy of all “uses and disclosures” of health information (as opposed to the nine “transactions” set out in the rule), noted that DHHS had failed to address many new technologies and business models. 70 Providers also complained that the establishment of new patient rights and imposition of procedural/disclosure obligations intruded unnecessarily into entities’ everyday business management and impeded patient treatment, research and quality improvement efforts by restricting information flows. 71 Finally, the industry argued that the new regulations rendered health care contracting unnecessarily complex and threatened the survival of the health information industry. 72

Uncertain interaction between HIPAA and preexisting privacy laws. While uncertainty “reigned supreme” as to HIPAA’s interaction with other applicable federal law, industry and state government representatives quarreled over the interpretation of regulatory language preserving “more stringent” state laws from HIPAA preemption. 73

Specific deficiencies. 74 Industry critics were unanimous in their outrage over DHHS’ apparent creation of a private right of action for individuals to recover, as third party beneficiaries to business partner agreements, from providers that engage in unlawful disclosure of protected information. 75 Varied criticism also

---


69 The regulations cover far more entities than the federal Privacy Act, HCFA’s Medical Records COPs, federal substance abuse record requirements, and state confidentiality laws. See Tomes, supra note 36, at 16; Waller, supra note 15, at 709. Moreover, the regulations’ protection of demographic and “billing, claims and related financial and administrative information” is a radical departure from federal and state precedent protecting medical record information. See Waller, supra note 15, at 709.

70 See supra note 67.

71 See id.

72 See id.


74 See Marks, supra note 38, at 803-05; HHS Hopes to Answer Industry Concerns In Final Version of HIPAA Privacy Regulation, 9 Health L. Rep. (BNA) No. 43, at 1666 (Nov. 2, 2000); Privacy Standards Need Clearer Definition, Congruity with HIPAA, BCBSA Says, 9 Health L. Rep. (BNA) No. 8, at 275 (Feb. 24, 2000); Page & Larios, supra note 73, at 8; Tomes, supra note 36, at 14-15.

75 See sources supra note 67.
focused on the vague definitions of "health care operations" and "minimum necessary" disclosures; frustration with the standards' short 2-year compliance period; confusion as to the standards' applicability to paper records; queries as to the extent to which covered entities were required to monitor business partners; concern with law enforcement's easy access to protected information; and uncertainty about the standards' application to ERISA plans. DHHS addressed many of these specific concerns in the final rule, discussed infra.

D. Final Privacy Rule

The final privacy rules, effective February 26, 2003, made numerous changes to the proposed rules above. The changes generally reflect DHHS's intent to balance individual privacy protection against specific quality, research and fraud protection concerns. DHHS has greatly expanded the types of protected information, the complexity of obligations, and the universe of entities covered by privacy rules, while (as in the proposed security rule) making some accommodations for the covered entities' peculiar structures and varied functions.

Since only the key provisions of the nearly 400-page rule are discussed herein, readers are advised to consult the statute and rule with regard to specific issues.

1. New/Modified Definitions

DHHS effected dramatic changes to the privacy rules in its revisions and additions to the privacy-specific "definitions" section. The most important of these changes was DHHS's revision of the definition of "protected health information" to include, for purposes of the privacy rule, all paper and oral (as well as electronic) protected health information. No doubt sensing the high likelihood of future legal challenges to this enormous expansion of the privacy rules' scope, DHHS

---

76 See sources supra note 67.

77 See 45 C.F.R. § 164.534 (2001). Under the final rule's transition provisions, covered entities may generally rely on consents, authorizations, or other express legal permissions obtained prior to the HIPAA compliance deadline. See id. § 164.532. With regard to activities related or unrelated to treatment, payment or health care operations or other purposes, covered entities may rely on pre-rule consents as to information previously created or received if the covered entity: (1) does not make any use or disclosure that is expressly excluded from the consent; (2) complies with all limitations in the consent. See id. With regard to research activities, covered entities may rely on pre-rule "consents" as to a specific research project if: (1) the entities' uses or disclosures are consistent with the "purpose" of the project and (2) the entities comply with all limitations in the consent. Proper "purposes" are defined by the scope of the pre-rule consent (i.e., specific or general consents). Covered entities qualifying under these transition provisions will be bound by any restrictions imposed after the final rule's effective date on new uses and disclosures of protected information. See id.

78 See 65 Fed. Reg. 82,462, 82,471 (2000). This balancing act reflects reality. While studies have shown that the public's fear of misuse of health information drives its unwillingness to allow unfettered disclosure of such information, the industry still requires access in order to serve public health needs. *EBRI Study Finds Conflict Between Privacy, Need for Data*, AH LA E-HEALTH L. & POL'Y REP., Dec. 21, 2000.

structured this revision so as to allow judicial severance of provisions addressing paper and oral information, rather than elimination of the entire definition. Other key definitional changes included (1) new definitions of “direct” and “indirect” treatment relationships, important for purposes of revised “permission” and notice provisions, discussed infra in subsections II(D)(2) and (3); (2) clarification of the definition of “health care operations,” incorporating an important exception for uses and disclosures between participants in “organized health care arrangements” and (3) the addition of three new definitions, “covered functions,” “plan sponsor” and “organized health care arrangements,” reflecting DHHS’s

80 See 64 Fed. Reg. 82,496 (2000).

81 Obviously, these new terms are opposites. Indirect treatment relationships involve the provision of treatment on orders of another provider, and the provision of services, products, diagnoses and results through another provider. 45 C.F.R. § 164.501. Direct treatment relationships are defined as non-indirect treatment relationships. See id. For example, radiologists and pathologists are considered to have indirect treatment relationships with patients, while outpatient pharmacists and Web-based providers have direct treatment relationships. 65 Fed. Reg. at 82,489, 82,492.

82 See 45 C.F.R. § 164.501; 65 Fed. Reg. at 82,494-95. Under both the proposed and final rules, covered entities that maintain protected health information may disclose it for their own health care operations, but not for the operations of a second covered entity. The final rule (1) adds to the list of proposed health care operations: certain business operations (planning, development, management and administration), due diligence by potential successor entities, internal grievance resolution activities, customer service activities not requiring disclosure of protected information of the customer; (2) fine tunes certain existing categories of “operations” (QA/QI not resulting in “generalizable knowledge,” student training, insurance activities, and preparation for legal activities); and (3) expands the scope of the rule to include (a) listed activities to the extent that the activities are related to the health care entities “covered functions” (not just “treatment and payment,” as under the proposed rule) and (b) disclosures for the operations of “organized health care arrangements” (defined in note 79, infra) in which the entity participates.” The definition adds new, albeit limited flexibility, in disclosures for fundraising and marketing activities. Given the allowance for disclosure to organized health care arrangements, the rule clarifies that the health care operations analysis is conducted separately from the “business associate” analysis, above. Thus disclosure of protected health information could be allowed under this rule to entities which are neither covered entities nor business associates.

83 See 45 C.F.R. § 164.501 (Covered functions are activities or functions that make an entity a “covered” health plan, health care provider or clearinghouse).

84 See id. (The privacy rules’ definition of “plan sponsor” was adopted from ERISA: “the employer or employee, or both, that establishes and maintains an employee benefit plan,” or if established by two or more employers, “the association, committee, joint board of trustees, or other similar group of representatives” that establish or maintain the plan.). As discussed infra, group health plans or plan insurers may disclose protected information to plan sponsors who conduct payment and health care operations activities on behalf of the group health plan if the requirements for group health plans in § 164.504(f)(1) are met.

85 See id. § 164.501 (2001). Organized health care arrangements are arrangements “involving clinical or operational integration among legally separate covered entities in which it is often necessary to share protected health information for the joint management and operation of the arrangement,” and where individuals “have an expectation that these arrangements are integrated and that they jointly manage their operations.” Arrangements “may necessarily involve the business associates of the covered entities and may involve the participation of the “plan sponsor” (defined below) to the extent that it is providing plan administration functions subject to the limits in § 164.504.” The definition explicitly includes (1) hospitals, where multiple providers may treat a patient by virtue of having been given privileges to do so; (2) joint enterprises among covered entities holding themselves out as participating in a joint arrangement and carrying out joint activities such as utilization review, QA/QI activities, or payment activities involving review of
increased focus on the privacy practices of complex business associations, discussed infra in subsection II(D)(4).

The final privacy rules also effected several changes through additions and revisions to the “general” definitions applicable to all HIPAA rules. The most important change was the substitution of the term “business associates” for that of “business partners.” These new entities, as well the corresponding revisions to business associate contract provisions, are discussed infra in section II(D)(5).

2. Rule of Nondisclosure; “Permission” Requirements/Exceptions; Additional Limitations

The final rules retain the general prohibition against covered entities’ disclosure of protected information and increase specific controls over permitted means of using and disclosing protected information.

Specifically, covered entities must now obtain one of three forms of individual “permission”—authorization, consent or agreement—for most uses and disclosures of protected information. Joint “permissions” are sanctioned under the “component entity” rules, discussed infra in section II(D)(4). The new permission structure dispenses with the proposed exception for uses and disclosures in cases of “treatment, payment or health care operations.” The authorization requirement, a carry-over from the proposed rule, applies to (1) uses and disclosures of protected information by other participants or a third party for the purpose of administering shared financial risk among participants (as with IPAs); (3) group health plans, and insurers or HMOs to the extent that they maintain plan participants' information; (4) group health plan[s] maintained by the same “plan sponsor” (defined below); and (5) combinations of group health plans maintained by the same sponsors, and insurers and HMOs to the extent that they maintain plan participants' information. See id.

An earlier definition of “business associates” was provided in the Electronic Transaction and Code Set rules, discussed infra in Part III. Other notable changes were the rules’ clarification of exemptions from the definitions of “health care” and “health plan,” as well as the adoption of the transaction rules’ definition of “health care clearinghouse” and “health care provider.” These changes are reflected in the definitions of these terms. See supra notes 10-12 and accompanying text.

See generally 45 C.F.R § 164.508; 65 Fed. Reg. 82,513-24 (2000) (to be codified at 45 C.F.R. § 164.506). Authorizations must conform with elements set out in § 164.508(c), applicable to all authorizations. Authorizations must also comply with § 164.508(d), (e) & (f) if requested by a covered entity conducting research that includes individual treatment (except as permitted by public policy); for its own uses/disclosures; or to obtain disclosure to the entity by third parties for purposes of treatment, payment or health care operations. Authorization may contain additional, non-required elements. Authorization may allow uses and disclosure for both covered entities and third parties. Authorizations may not be combined with other legal documents, except for three “compound” documents (examples provided in rule): research authorizations combined with consent for treatment; authorization for the use of psychotherapy notes for multiple purposes; and authorization for the use of protected information other than psychotherapy notes, provided that treatment, payment, enrollment or eligibility was not conditioned on authorization. A “compound” authorization must also comply with § 164.508(b)(3). Authorization may not be required as a condition of treatment, payment, and eligibility/enrollment, except (1) for treatment, except for research and treatment given for the sole purpose of providing information to a third party (ex: fitness exam; life insurance physicals); (2) for payment, except for health plans to “determine payment of the claim;” (3) for eligibility/enrollment, exception for “purposes of eligibility or enrollment determinations relating to the individual or for underwriting or risk-rating determinations.” An authorization may be revoked in writing at any time, except for (1) uses and disclosures made in reliance on authorization and (2) insurance authorizations. See id.
psychotherapy notes to carry out treatment, payment or health care operations and (2) any other lawful uses or disclosures of protected information that are not otherwise permitted or required by the rules as discussed in this subsection or subsection II(D)(4). Health care providers maintaining direct treatment relationships with individuals must obtain their written “consent” to use or disclose protected information (other than psychotherapy notes) for treatment, payment or health care operations. Finally, covered entities must orally provide patients with an opportunity to agree to or “opt out” of uses or disclosures of protected information (1) for patient directories, to clergy, or to other persons who ask for the individual by name or (2) to an individual’s caregivers for purposes of

---

88 See 45 C.F.R. § 164.501. “Treatment” is defined as:
the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Id.

89 See id. “Payment” is defined as:
(1) [t]he activities undertaken by [a] health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan[,] or [a] covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) [t]he activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: [n]ame and address; [d]ate of birth; [s]ocial security number; [p]ayment history; [a]ccount number; and [n]ame and address of the health care provider and/or health plan.

Id.

90 See supra note 67.

91 See generally 45 C.F.R. § 164.506; 65 Fed. Reg. 82,462, 82,509-13 (2000). A “consent” must conform to the six content requirements of §164.506(c) and be accompanied by a notice of privacy practices pursuant to §§164.503(b), 520. Consent may cover one or all of the three “purposes” to which it is addressed. Consent may be rolled into a single document containing other types of legal permissions, provided that health information provisions are “visually and organizationally separate” and are separately signed and dated. Consent may also be rolled into a research “authorization,” but not any other authorization. §§164.506(b)(4), 508(f). Consent alone (i.e., without an “authorization”) allows use and disclosure only by the covered entity, except in cases of joint consents obtained and except in the case of business associates acting “on behalf of” the covered entity. Providers may require consent for treatment. Health plans may require consent for purposes of treatment, payment or health care operations, but only if they seek consent in conjunction with enrollment (i.e., not retroactively). Upon revocation of consent, processing of protected information must cease, but so may the individual’s treatment and enrollment in a health plan. Revocation of joint content, discussed infra in subsection II(D)(4), requires the receiving entity to notify other affected covered entities.
notifying or assisting in notifying such caregivers of the individual’s status.\footnote{See generally 45 C.F.R. § 164.510; 65 Fed. Reg. at 82,521-24 (2000). Where oral communication is impossible, agreement or objection may be reasonably inferred from the surrounding facts and circumstances; where inferred, the minimum necessary information may be disclosed to proper persons, if disclosure is consistent with good professional judgment. For incapacitated patients or in emergency situations, the rules allow non-agreed-to disclosure to a patient directory if disclosure is determined to be in the patient’s best interests. Agreement is not required for necessary disclosures to certain organizations engaged in disaster relief.}

There are numerous exceptions to the “permission” rules. While retaining proposed exceptions for uses and disclosures for purposes consistent with public policy,\footnote{See 45 C.F.R. §§ 164.502, 512. This section sets out non-exclusive public policy exceptions for uses and disclosures by covered entities (1) as “required by law” (defined in § 164.501); (2) to certain persons or entities involved in public health or FDA-regulated activities, to persons who may have been exposed to a communicable disease where authorized by law in the conduct of a public health intervention or investigation, or, with proper notice, to employers where required by workplace safety laws; (3) about victims of abuse, neglect or domestic violence, as authorized or required by law or individual consent, and subject to certain notice provisions (new); (4) for limited health oversight activities, including voluntary compliance disclosures and fraud investigations (distinguished in § 512(d)(2) from “law enforcement” activities); (5) pursuant to judicial/administrative order or, subject to certain limitations, a private party’s subpoena or discovery request; (6) for law enforcement purposes (not a new affirmative requirement; privacy advocates note that an impartial hearing is not required); (7) about decedents, or other persons in the decedent’s medical record, to coroners, medical examiners, funeral directors, and hospitals performing such functions; (8) for purposes of cadaveric organ, eye or tissue donation (if donor living, need consent); (9) for research, subject to limitations including a properly-documented IRB authorization “waiver,” right of individual access, and other applicable regulations (Common Rule, FDA human subjects regs); (10) to avert a “serious and imminent” threat to individual or public health and safety (some overlap with law enforcement, as with potentially violent patients or prison escapees, but not intended to create a duty to warn); (11) pursuant to specialized government functions, including certain required inter-agency information sharing by “covered” government programs providing public benefits; (12) to employers for workers compensation or other similar purposes (new). See id. The final rule eliminates proposed exceptions for (1) government (or private) health data systems and (2) banking/payment processes. These exceptions do not preempt “state or other restrictions.” 65 Fed. Reg. 82,531. (Author Commentary).} the final rules add exceptions for disclosures to individuals or their personal representatives (formerly subject to authorization rules),\footnote{See id. § 164.514(e); 65 Fed. Reg. at 82,545-46.} as well as for certain marketing,\footnote{See 45 C.F.R. § 164.514(f); 65 Fed. Reg. at 82,546.} fundraising\footnote{See 45 C.F.R. § 164.514(g); 65 Fed. Reg. at 82,546.} and underwriting\footnote{See 45 C.F.R §§ 160.300-312 (formerly 45 C.F.R. § 164.522); 65 Fed. Reg. at 82,487.} activities. Disclosure will be required if requested or mandated by an appropriate entity for compliance or enforcement purposes.\footnote{Note that uses and disclosures may also be limited either by agreement (as in business associate contracts, or in the restriction agreements and confidentiality requests discussed infra at note 115), or by the terms of any notice accompanying solicitations of individual “permission.”}

Additional limitations on the use and disclosure of information include the “minimum necessary” disclosure and “verification” requirements.\footnote{See 45 C.F.R. §§ 164.502, 512. This section sets out non-exclusive public policy exceptions for uses and disclosures by covered entities (1) as “required by law” (defined in § 164.501); (2) to certain persons or entities involved in public health or FDA-regulated activities, to persons who may have been exposed to a communicable disease where authorized by law in the conduct of a public health intervention or investigation, or, with proper notice, to employers where required by workplace safety laws; (3) about victims of abuse, neglect or domestic violence, as authorized or required by law or individual consent, and subject to certain notice provisions (new); (4) for limited health oversight activities, including voluntary compliance disclosures and fraud investigations (distinguished in § 512(d)(2) from “law enforcement” activities); (5) pursuant to judicial/administrative order or, subject to certain limitations, a private party’s subpoena or discovery request; (6) for law enforcement purposes (not a new affirmative requirement; privacy advocates note that an impartial hearing is not required); (7) about decedents, or other persons in the decedent’s medical record, to coroners, medical examiners, funeral directors, and hospitals performing such functions; (8) for purposes of cadaveric organ, eye or tissue donation (if donor living, need consent); (9) for research, subject to limitations including a properly-documented IRB authorization “waiver,” right of individual access, and other applicable regulations (Common Rule, FDA human subjects regs); (10) to avert a “serious and imminent” threat to individual or public health and safety (some overlap with law enforcement, as with potentially violent patients or prison escapees, but not intended to create a duty to warn); (11) pursuant to specialized government functions, including certain required inter-agency information sharing by “covered” government programs providing public benefits; (12) to employers for workers compensation or other similar purposes (new). See id. The final rule eliminates proposed exceptions for (1) government (or private) health data systems and (2) banking/payment processes. These exceptions do not preempt “state or other restrictions.” 65 Fed. Reg. 82,531. (Author Commentary).} The final “minimum necessary” rules, applicable to all “covered” and some “public policy” activities, modify the proposed requirement that covered entities use or disclose
only the minimum amount of information necessary for a particular purpose.\textsuperscript{100} For routine disclosures, covered entities may now implement prophylactic policies and procedures \textit{in lieu of} reviewing each use or disclosure for compliance; all other requests must be individually reviewed.\textsuperscript{101} The final "minimum necessary" rule excepts uses and disclosures for treatment purposes or which are required data elements rules under the final electronic transactions standards rules, and it retains proposed exceptions for disclosures to protected individuals, "authorized" disclosures, or disclosures for HIPAA compliance purposes.\textsuperscript{102} Moreover, covered entities may rely that requests made by other covered entities, certain "professionals," public officials, and certain research entities are for "minimum necessary" information.\textsuperscript{103} As to the verification requirement, the final rule provides that covered entities must verify and document the identity and legal authority of information requestors prior to disclosure,\textsuperscript{104} if the requestors' identity is unknown\textsuperscript{105} or their legal authority to make a request is uncertain.\textsuperscript{106}

3. Required Notice Accompanying Individual Permission

In an effort to increase individuals' awareness of the possible uses and disclosures of protected information,\textsuperscript{107} the final rules require that covered entities soliciting individuals' "permission" also provide\textsuperscript{108} such individuals with notice of (1) the covered entities' privacy practices\textsuperscript{109} and (2) individuals' right to request

\begin{flushright}
\textsuperscript{100}Compare 45 C.F.R § 164.514(d) (final), \textit{with} 45 C.F.R § 164.506(b) (proposed).
\end{flushright}

\begin{flushright}
\textsuperscript{101}See 45 C.F.R § 164.514(d).
\end{flushright}

\begin{flushright}
\textsuperscript{102}See id. § 164.502(b)(2).
\end{flushright}

\begin{flushright}
\textsuperscript{103}See id. § 164.514(d)(3)(iii).
\end{flushright}

\begin{flushright}
\textsuperscript{104}Under the final rule, the identity of requesting \textit{users} need not be verified. \textit{See} 65 Fed. Reg. 82,462, 82,547 (2000).
\end{flushright}

\begin{flushright}
\textsuperscript{105}Individuals' identity may be "known" by their place of business, address, fax, actual name, or documentation submitted with the request. \textit{See} 65 Fed. Reg. at 82,546.
\end{flushright}

\begin{flushright}
\textsuperscript{106}See 45 C.F.R. § 164.514(h) (2001); 65 Fed. Reg. at 82,546-47.
\end{flushright}

\begin{flushright}
\textsuperscript{107}See 65 Fed. Reg. at 82,474.
\end{flushright}

\begin{flushright}
\textsuperscript{108}Notice distribution requirements vary according to whether a covered provider has a direct or indirect treatment relationship with the individual. \textit{See} 45 C.F.R. § 164.520(c). If direct, notice must be (1) posted and available on site and (2) delivered as of the first personal or electronic service delivery after the compliance date (unless a provider opts to send notice to all patients at once). \textit{See id.} If indirect, notice must be provided only if requested. Notice may be given electronically, if an individual has agreed to electronic delivery and notice is also provided to the individual at the first request for service. \textit{See id.} Note that the final rule also addresses web sites, requiring that privacy notices be posted thereupon. \textit{See id.} § 164.520(c)(3).
\end{flushright}

\begin{flushright}
\textsuperscript{109}The final rule mandates only general notice of privacy practices, as opposed to the proposed detailed disclosure of all policies and procedures, but specifically requires a listing of (1) a specific notice "header," 45 C.F.R. § 164.520(b)(1)(i); (2) specifically intended uses and disclosures, \textit{see id.} § 164.520(b)(1)(ii)(iii); (3) individual rights, and the methods of exercising such rights, \textit{see id.} § 164.520(b)(1)(iv); (4) the covered entities duties, \textit{see id.} § 164.520(b)(1)(v); (5) complaint information; (6) contact persons, \textit{see id.} § 164.520(b)(1)(v); and (7) the effective date of the notice, \textit{see id.} § 164.520(b)(1)(viii). The rule also lists several optional elements. \textit{See id.} § 164.520 (b)(2)(2001). Covered
certain privacy restrictions on the use and disclosure of protected information. The final rule eliminates a proposed “model” notice, and promises only “further guidance” as to proper language. Furthermore, the notice provision does not eliminate the need for compliance with other federal notice requirements (including the forthcoming final “E-signature” rule) or “more stringent” state notice requirements, raising the specter of multiple notices in connection with covered entities’ varied functions. Finally, the final privacy rules somewhat complicate matters by separately regulating notice to group health plan beneficiaries. Covered “component entities” may gain some regulatory relief, however, under “joint notice” provisions discussed infra at section 4(d).

4. Expanded Rules Governing Uses and Disclosures in Complex Business Associations: Organized Health Care Arrangements, entities must retain copies of all notices provided. See generally 45 C.F.R. §§ 164.502, 520; 65 Fed. Reg. at 82,552-554. The rules provide for two types of requests: (1) restrictions on uses and disclosures and (2) confidentiality requests. First, the final rule extends proposed provisions allowing the individual to request that covered entities restrict uses and disclosures of protected information for treatment, payment or health care operations. See id. Providers need not agree to such restrictions, but if they do agree, they must document and abide by such restrictions. See id. Covered entities are not required to disclose the existence of restrictions in conjunction with disclosures of other unrestricted information. See id. Restrictions will not apply (1) in “rare” cases where disclosure to providers is necessary for emergency treatment, provided that the disclosing entity requests that the provider make no further disclosures, or (2) to certain “excepted,” “required,” or “agreed-to” uses and disclosures, discussed supra. Second, under new final rule provisions, providers and health plans must accommodate individuals’ reasonable requests as to the means or location of communication of protected information, unless the individual has failed to provide information as to (1) how payment, if any, will be handled or (2) alternative locations for or means of communication. See id. Health plans must comply only if all or part of the information could endanger the individual. See id. The reasonability of a request must otherwise be determined solely on the basis of the difficulty of administrative compliance therewith (i.e., not on the basis of either the merits of, or the individual’s refusal to justify, the request). See id. Note that covered entities may terminate all restrictions with an individual’s oral (documented) or written agreement; without such agreement, an entity may terminate restrictions only as to information created or received after informing the patient of intent to terminate. See id.

See generally 45 C.F.R. §§ 164.520(a)(2); 65 Fed. Reg. 82547. Under the final rules, individual insureds have a right to notice from (1) group health plans directly offering benefits to self-insured entities; and (2) insurers or HMOs providing benefits to group health plan beneficiaries. See id. Notice must be provided upon enrollment and within 60 days of revision and “no less than once every three years” (as opposed to “every three years” under the proposed rule). See 45 C.F.R. § 164.520(c)(1)(B), (c)(1)(C), (c)(1)(ii). Each dependent need not receive notice if provided to the insured, and where multiple notices are available, notice need be only that which is relevant to the particular insured. See id. Also, group health plans must meet specific “distribution” requirements set out in the rule. However, certain group health plans offering “insured” benefits (i.e., through HMOs or insurers described in category (2), above) may be either (1) required to only “maintain” notice and provide it “upon request,” and will not be subject to distribution requirements or (2) exempt from the notice requirements altogether, if they receive only “summary” or otherwise exempt insurance information. See 45 C.F.R. § 164.520 (a)(2)(ii)(A), (a)(2)(ii)(B), (a)(2)(iii).
The preamble to the proposed rules required that in order for large organizations encompassing legally distinct "component entities" to avoid regulation as covered entities, they must erect firewalls to insulate protected information in possession of component entities from improper use by or disclosure to the larger organization. The final rule applies the firewall requirement to "hybrid" entities, or covered entities performing covered functions that are not the entities’ primary function (e.g., an employer with a health clinic, or an insurer offering both health and non-health benefits). Specifically, hybrids must erect firewalls “to protect against ... improper use or disclosure within or by the organization.” DHHS expects that firewalls may affect covered entities’ record-keeping and accounting practices.

However, the direct regulation of certain group health plans’ disclosures deviates significantly from the “component entity” approach. While most group health plans are deemed to be “covered entities,” the plans’ own sponsors (such as plan beneficiaries’ employers) are not, even when designated in plan documents as plan “fiduciaries” requiring access to protected beneficiary information in order to properly oversee the operation and administration of the plan. Abandoning the proposed “component entity” approach to regulating disclosures by group plans to their sponsors, the final rule imposes direct limitations on the flow of protected information to plan sponsors in an effort to preclude the use of protected information “for employment-related functions or for other functions related to employee benefit plans or other benefits.”

Final “multiple covered function entity” rules govern uses and disclosures}

---

115 See supra note 77.
117 45 C.F.R. § 164.504(c)(2).
118 See 65 Fed. Reg. at 82,502-03. In the examples above, covered health records must be segregated from business-related or records pertaining to “excluded” benefits. Additionally, the entity must comply with all “compliance and enforcement,” policy and procedure, and documentation requirements of the rule. See id.
119 Plans with less than 50 beneficiaries are not “covered entities” for purposes of the rule. See 45 C.F.R. § 160.103.
120 See supra note 77.
121 45 C.F.R § 164.504(g); 65 Fed. Reg. at 82,507-09. Specifically, the rule requires amendments to plans’ governing documents that (1) limit the circumstances under which protected information may be used or disclosed; (2) require the erection of firewalls; and (3) identify sponsor employees who receive plan-related information. See id. Plan sponsors must certify the amendment and compliance with the rule (removing this burden from HMOs or insurers). See id. The rule severely restricts sponsors’ “administration” activities and access to information from the plan or HMOs or insurers. Finally, the rule allows, subject to notice provisions, plans’ provision to sponsors of “summary information” for the purpose of soliciting premium bids, deciding whether to change benefits offered, or modifying, amending or terminating the plan. See id.
by “single entities, affiliated entities, or other arrangements” to the extent that they combine to perform multiple covered functions.\textsuperscript{122} Such entities may only use or disclose the protected information (1) of an individual involved in the particular function (2) in a manner consistent with the rules applicable to such function.\textsuperscript{123}

Lastly, but perhaps most importantly, both “organized health care arrangements” and “affiliated entities,” or organizations that are under common ownership or control,\textsuperscript{124} are permitted in the final rules to designate themselves “single entities” for purposes of joint consent.\textsuperscript{125} In addition, organized health care arrangements may also provide joint notice of information practices;\textsuperscript{126} however, affiliated entities may provide joint notice only if they elect against designation as a single entity for purposes of consent and otherwise qualify as organized health care arrangements.\textsuperscript{127} In either case, joint notice will be permitted only if it conforms with general content requirements, \textit{supra}; identifies the entities and sites covered by the notice; and, where applicable, discloses the fact that participating entities will share information for purposes of treatment, payment or health care operations related to the arrangement.\textsuperscript{128}

5. Business Associate Rules

As discussed above, the final privacy rule replaces the proposed definition of “business partners” with a new term, “business associates.” A business associate is any person or entity, including a covered entity, that

(1) “performs, or assists in the performance of,” certain functions or activities\textsuperscript{129} involving the use or disclosure of individually identifiable health information “on behalf of” a covered entity or organized health care arrangement in which the covered entity

\begin{itemize}
\item \textsuperscript{122} 45 C.F.R. § 164.504(g); 65 Fed. Reg. at 82,509.
\item \textsuperscript{123} See 45 C.F.R. § 164.504(g); 65 Fed. Reg. at 82,509. Thus, the preamble notes, a health system may share information about a hospitalized patient with the patient’s health plan only if the patient is a plan member.
\item \textsuperscript{124} See 65 Fed. Reg. at 82,503 (“Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.”).
\item \textsuperscript{125} See \textit{supra} note 77 (“organized health care arrangements”); 45 C.F.R. § 164.504(d)(1) (“affiliated entities”).
\item \textsuperscript{126} See 45 C.F.R. § 164.520(d).
\item \textsuperscript{127} See 65 Fed. Reg. at 82,552.
\item \textsuperscript{128} See 45 C.F.R. § 164.520(d)(2)(i)(ii)(iii).
\item \textsuperscript{129} Business associate functions or activities include “claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or [a]ny other function or activity regulated by this subchapter [45 C.F.R. Subtitle A, Subchapter C].” 45 C.F.R. § 160.103(i)(A)(B).
participates,\textsuperscript{130} or .

(2) "provides" certain services\textsuperscript{131} "to or for" a covered entity or organized health care arrangement in which the covered entity participates, which services involve the disclosure of protected health information "from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person."\textsuperscript{132}

The definition of business associate explicitly excepts certain internal elements of covered entities, including their "workforce"\textsuperscript{133} or, in the case of an organized health care arrangement, their "participants."\textsuperscript{134} Certain other parties acting "on their own behalf" are not considered business associates.\textsuperscript{135} Thus, DHHS would also exclude financial institutions' processing of consumer-instituted transactions; providers' disclosures to a plan for payment purposes; a hospital's grant of physician privileges; an HMO's or insurer's provision of insurance to group health plans; and disclosure of information to oversight agencies acting on behalf of federal programs (exempting, for instance, HCFA's disclosures to OIG).\textsuperscript{136} Finally, a business associate contract is not required for "conduits" of protected information that access protected information only on a random or infrequent basis, such as the postal service and "private couriers or their electronic equivalents."\textsuperscript{137}

Mandatory business associate contract rules, only slightly modified in the

\textsuperscript{130} DHHS's reference to "organized health care arrangements" recognizes that business associations arise in the course of "joint arrangements for the delivery or financing of health care," in which persons are contracted to perform functions or provide services for the joint arrangement. This concept is designed to be consistent with the modified definition of "health care operations," which includes joint operations. However, a non-covered entity's mere participation in a joint arrangement does not transform it into either a covered entity or a business associate unless it is actually performing the above "functions or activities" or providing specified services "on behalf of" such entities. See 65 Fed. Reg. at 82,476.

\textsuperscript{131} Covered services include: "legal, actuarial, accounting, consulting, data aggregation, . . . management, administrative, accreditation, or financial services." 45 C.F.R. § 160.103. Data aggregation means the combination by a business associate (in its capacity as such) of unaffiliated entities' protected health information "to permit data analyses that relate to the health care operations" of each entity. 45 C.F.R. § 164.501. Its inclusion as a "specified service" clarifies the ability of certain covered entities (such as state hospital associations) to contract with other entities (such as member hospitals) for purposes of QA and comparative analyses involving protected information of more than one covered entity. 65 Fed. Reg. 82,475.

\textsuperscript{132} 45 C.F.R. § 160.103.

\textsuperscript{133} "Workforce means 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.

\textsuperscript{134} See id.

\textsuperscript{135} See 65 Fed. Reg. at 82,476.

\textsuperscript{136} See id.

\textsuperscript{137} See id.
final rule, continue to ensure that covered entities can disclose protected information to business associates only upon receipt of “satisfactory assurances” that the associates will handle the information in a manner consistent with both applicable law and the terms and purposes of the business association. Important exceptions to the contracting requirement include disclosures by health care providers for “treatment” purposes; by group health plans or plan insurers to plan sponsors (subject to the “group health plan” restrictions discussed in subsection 4(d), supra); by certain “government health plans providing public benefits;” and by financial institutions processing consumer-conducted financial transactions.

As under the proposed rule, business associate activities relating to protected health information are imputed to the entity or arrangement on whose behalf a business associate is acting. However, DHHS has partially removed the specter of private privacy-related litigation by eliminating the much-criticized requirement that protected individuals be named in business associate contracts as intended third party beneficiaries. Furthermore, sanctions may be imposed only if a covered entity or arrangement has culpable knowledge of business associate’s wrongdoing. In a significant departure from the proposed requirement that covered entities continuously monitor their associates’ activities, covered entities must now investigate a potential violation if presented with a complaint or other “substantial and credible” information of breach. Furthermore, termination is required “when feasible” after a failed attempt to cure such breach; however, a breached contract may not be allowed to continue merely for a covered entity’s “convenience.”

---

138 See id. at 82,503-07. The final rules clarify that a contract is required even if a business associate is a covered entity, that conforming “master” agreements apply to all signatories; and that a contract may be more restrictive than rules. See id. The final rule also (1) allows use/disclosure of protected information from multiple sources, including individual covered entities, organized health care arrangements, or “joint” entities needing “payment” services, for purposes of “data aggregation” by business associates (formerly prohibited because this activity cannot otherwise be performed by covered entities); (2) requires business associates to make information available for amendment, accounting purposes; (3) imposes “more flexible” requirements for post-contract treatment of information; (4) clarifies that business associates must only ensure conformity to contract terms by delegees assuming (listed) responsibilities considered those of business associates, thereby excepting from business associate oversight the delegation of non-associate “functions, activities and services” as well as generally excepted uses or disclosures; (5) allows for alternative means of satisfying the “satisfactory assurances” requirement by government agencies or in situations where a business association is required by law; and (6) allows business associates to use “professional judgment” to determine the extent to which uses and disclosures are necessary to carry out contractual functions while maintaining confidentiality. See 65 Fed. Reg. at 82,503-07.

139 See 45 C.F.R. § 164.504(e) (2001).

140 45 C.F.R. § 164.502(e)(1)(ii); 65 Fed. Reg. at 82,504-05.

141 See 65 Fed. Reg. at 82,476.

142 Culpable knowledge arises only if a covered entity discovers or had reason to know of a business associate’s material breach of its contract and fails to take reasonable steps to cure the breach or terminate the contract. See id. at 82,505.

143 Id.
6. Individual Rights

Right of access. As in the proposed rule, individuals continue to have a right to request timely\textsuperscript{144} access\textsuperscript{145} to all non-expected\textsuperscript{146} information contained in a "designated record set,"\textsuperscript{147} including summaries and underlying information.\textsuperscript{148} The rule provides eight grounds for denial\textsuperscript{149} of access requests, three of which are "reviewable."\textsuperscript{150}

Right of Amendment. The final rule clarifies that individuals have a right to request that covered entities amend (but not correct) information contained in a designated record set.\textsuperscript{151} Covered entities may require that amendment requests be in writing and supported by specific reasons for amendments;\textsuperscript{152} covered entities that provide individuals with prior notice of these requirements may ignore

\textsuperscript{144} See 45 C.F.R. § 164.524(b)(2), (c)(3).

\textsuperscript{145} Under the new rule, covered entities need not reproduce information in requested formats that are not "readily obtainable," but must always produce a readable hard copy or use an alternative, agreed-upon format. See id. § 164.524(c)(2). Note that the rule also provides that reasonable, cost-based fees may be charged for copies (including labor and supplies associated with copying) and postage. See id. § 164.524(c)(4) (2001).

\textsuperscript{146} Excepted information includes (1) psychotherapy notes, (2) information compiled in anticipation of a legal proceeding (but not the underlying information), and (3) disclosures prohibited by or exempted from the Clinical Laboratory Improvements Act. See id. § 164.524(a)(i)(ii)(iii). Also, the right will not apply to health care clearinghouses acting as business associates. See id. § 164.500(b). See also supra note 138.

\textsuperscript{147} The final rule expands the scope of accessible information by broadening the definition of "designated record set." See 45 C.F.R. § 164.501. Generally, the new definition allows access to any information use to make decisions about individuals, but not information used for other purposes, such as quality control or peer review analysis. See 65 Fed. Reg. at 82,554.


\textsuperscript{149} Denials must conform to 45 C.F.R. § 164.524(d).

\textsuperscript{150} The final rule sets out five non-reviewable grounds for denial of access to (1) information subject to the three exceptions, see supra note 132; (2) certain information requested by inmates of correctional facilities, (3) information obtained by a covered provider in the course of research which includes treatment of patients, provided that the individual has agreed to the denial as a condition of participation and received notice that his/her right of access will be reinstated upon completion, (4) information subject to the Privacy Act, (5) information obtained from someone other than a provider by a covered entity under a promise of confidentiality, that would reveal the source of the information if access were granted. 45 C.F.R. § 164.524(a)(2) (2001). Individuals may request a timely review by certain health care professionals (see id. § 164.524(d)(4)) of denials of access to information that, in the judgement of such a professional, is "reasonably likely to endanger the life or physical safety" of (1) the requesting individual or another person (for example, if the individual displays suicidal homicidal or otherwise violent tendencies), (2) a person other than the requesting individual who is referenced in the information, or (3) the individual or other person referenced in the information, as a result of a request by the "personal representative" of the individual. See id. § 164.524(a)(3).

\textsuperscript{151} See 45 C.F.R. § 164.526. As with the right of access, the right of amendment does not apply to information created or received by health care clearinghouses acting as business associates. See id. § 164.500(b).

\textsuperscript{152} See id. § 164.526(b)(1).
Denial of amendment requests is appropriate if properly made and the covered entity either (1) did not create the record (unless there is a reasonable basis to believe that the record’s originator is no longer available to act on amendment) or (2) determines that the disputed information is “reasonably accurate and complete.”

Right to an Accounting. Individuals have a right to an accounting of up to six years of protected information disclosures by covered entities or business associates, provided that such disclosures were not for treatment, payment or health care operations or otherwise excepted. Accounting requests will likely impose significant staffing and administrative burdens for covered entities, given the public’s intense interest in accountability, the enormous number of transactions now subject to review for accounting/exception purposes, and the rule’s extensive accounting documentation provisions.

7. Overall Compliance with the Final Rule; Required Administrative Procedures

While privacy advocates have generally cheered the publication of the final privacy rules, they expressed specific concerns with the rules’ (limited)

154 Requests for amendment require some action (acceptance/denial, in whole or in part) within 60 days of the request, with possibility of a one-time 30-day extension following a written explanation for the delay. See 45 C.F.R. § 164.526(b)(2) (2001). Both acceptance and denial must conform with the rule. See id. § 164.526(c),(d).
155 Id. § 164.526(a)(2). As to the latter grounds for denial, DHHS notes: “Perfect records are not required.” 65 Fed. Reg. at 82,558.
156 An accounting must be provided no later than 60 days (increased from 30) after a request (with possibility of a one-time 30 day extension following a written explanation for the delay); covered entities are “encouraged” to respond appropriately to requests for expedited accounting. See 45 C.F.R. § 164.521(c)(1) (2001); 65 Fed. Reg. at 82,550. Individuals have a right to 1 free accounting per 12 month period, but a reasonable, cost-based fee may be charged for subsequent accountings following notice to the individual. See 45 C.F.R. § 164.521(c)(2). The rule contains specific provisions pertaining to content, including final rule additions pertaining to covered entities’ obligations to provide individuals with “reasonable” information as to the basis for disclosure (rather than produce the actual request), and allowing summary accounts of “recurrent” disclosures (i.e., regular disclosures of the same information or multiple disclosures to the same entity). See 45 C.F.R. § 164.528(b)(2)&(3).
158 See id. § 164.528(b)(1).
159 See id. § 164.528(a)(1)(i).
160 Notable exceptions from the rule include disclosures to the individual; disclosures for facility directories, to caregivers or for other notification purposes covered by § 164.510; disclosures made prior to the rule’s compliance date; disclosures to health oversight and law enforcement agencies during the time period (as specified by the agencies) that disclosure would impede their official activities. See id. §§ 164.528(a)(1)(ii)-(vi), (2).
161 See id. § 164.528(d) (documentation requirements).
marketing and fundraising exceptions, as well as their allowance of law enforcement access without a court order. Covered entities continue to complain about the rules’ lack of uniformity with existing and future state privacy rules, as well as their enormous cost. One commentator has offered a vision of legal battles to come by arguing that Congress improperly delegated its legislative authority to DHHS by requiring DHHS to write the privacy rules in the absence of congressional action. Some industry participants contend that DHHS has exceeded its statutory authority, and have announced that they will push Congress and President Bush to either eliminate or modify the most burdensome requirements and standards.

Until changes are made, covered entities must focus on compliance with the rules as currently written. First, covered entities must seek a legal briefing on the applicable provisions of the privacy rule. Second, any risk analysis must, for privacy rule purposes, (1) identify excepted information, uses and disclosures, and entities, (2) categorize the circumstances and types of permission required for individual covered entities’ unique uses and disclosures, (3) identify the appropriate type and content of notice, and (4) account for individual rights. Third, as above, covered entities must conduct a thorough review of “business associate” contracts and revise non-compliant contracts per the final rule.

The privacy rules’ “administrative procedure” provisions contain additional compliance directives. As in the security rule, covered entities or groups of covered entities must designate, and document the designation of, a privacy official and contact person, and include the names of such privacy personnel in its privacy notice. Second, covered entities must adopt and revise

---

162 See supra text accompanying notes 75, 87-88.
164 Data privacy, including compliance with both Graham-Leach-Bliley and HIPAA, will continue to be a top legislative issue in the coming year. See Privacy Issues, Mandates to Dominate State Legislative Agendas in 2001, HIAA Says, 10 Health L. Rep. (BNA) No. 4 (Jan. 25, 2001).
165 See discussion supra note 25.
166 William G. Schiffbauer, Congress Impermissibly Delegated Law-Writing Power to Executive Branch in Privacy Rule, 10 Health L. Rep. (BNA) No. 4, at 158 (Jan. 25, 2001). Also, as noted above, DHHS itself implicitly acknowledged that it may have exceeded its regulatory authority in expanding the rules’ coverage to protected health information in any form. See id.
167 See id.
169 See id. § 164.530(a).
170 See id. § 164.530(i). Note the special requirements for changes relating to privacy notices. See id. § 164.530(i)(2)(ii), (4). Moreover, the final rule expands the proposed scope of complaint procedures to include violations of an entity’s privacy practices, as well as violations of the rule.
privacy policies and procedures as required by the privacy rules. Privacy policies and procedures may take into account the peculiar characteristics of particular covered entities, but must (1) set forth sanctions for privacy and notice violations (except by whistleblowers and business associates, or for purposes of compliance and enforcement activities), (2) establish complaint procedures, and (3) establish documentation and record retention procedures. Privacy practices must also be incorporated into any notice accompanying requests for patient permission. Third, entities must implement certain safeguards to protect against proscribed uses and disclosures and/or inadvertent disclosures to unintended recipients. The final rule combines proposed security safeguards (designed to complement standards under the proposed security rule, applicable to electronic information) into a single, nonspecific standard that works in tandem with the “minimum necessary” rule above. Fourth, initial workforce privacy policy and procedure training must be completed by the effective date of the rule, and new member training (and training on new rules) must occur within a reasonable time.

III. ELECTRONIC TRANSACTION AND CODE SET STANDARDS

A. Statutory Background

HIPAA requires DHHS, working in conjunction with certain “standard-setting organizations,” to do the following:

Adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for-

---

171 See id. § 154.530(i).
172 See 45 C.F.R. § 154.530(i)(1).
173 Covered entities must mitigate the effects of any known violations and refrain from intimidating or retaliatory acts against complainants. See id. §§ 164.530(f), (g).
174 Covered entities may not require individuals to waive their rights to file a complaint as a condition of treatment, payment, enrollment or benefit eligibility. See id. § 164.530(h).
175 The rule requires written documentation by all covered entities (with some exception for certain group health plans) of (1) compliance policies and procedures in any form, or changes thereto, (2) reservation of rights to change such policies or procedures, (3) changes due to new law, and (4) changes in privacy practices in individual notice. Documentation must be retained for six years. See id. § 164.530(j).
176 See id. § 164.530(c).
177 See 45 C.F.R. § 164.530(c).
178 See id. § 164.530(b).
179 42 U.S.C. §§ 1320d(8), 1320d-1(c), (f), (g) (2000).
HIPAA BECOMES REALITY

(A) [certain] financial and administrative transactions;\(^{180}\) and

(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.\(^{181}\)

B. Final Electronic Transaction and Code Set Rules

DHHS's final standards for electronic transactions and code sets will become effective as to all covered entities (except small health plans) on October 16, 2002. The new standards are distinct from the privacy and security standards in two ways: (1) they are more specific in focus and (2) they govern data transmission, as opposed to only data protection.

The rules' intent is to standardize certain payment or claims-related transactions\(^{182}\) in a manner similar to that employed in the banking industry.\(^{183}\) Presently there are more than 400 different formats required by payors related to these transactions. This standardization is expected to save billions of dollars and was the heart of HIPAA's administrative simplification provisions until overshadowed by privacy concerns.

\(^{180}\) See infra note 191 and accompanying text.


These rules require covered entities, their business associates and trading partners to use standardized transaction formats, data content, data elements, and code sets (where applicable) when conducting eight "covered transactions." Technical assistance for every standard transaction is provided through "implementation guides," available as provided in the rule. The rules also modify and adopt existing code sets for use at the time services are rendered.

---


185 See 45 C.F.R. § 162.923(c) (2001).

186 "Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement." Id. § 160.103. Such agreements may not contain provisions contrary to the electronic transaction rule. See id. § 162.915.

187 "Format" means "data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction." Id. § 162.103.

188 "Data Content" includes "all the data elements and code sets inherent to a transaction, and not related to the format of transaction." 45 C.F.R. § 162.103. "Data elements" are "the smallest named unit[s] of information in a transaction." Id. "Code sets" are "any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes." Id. At the heart of the standardization of data content is the concept of the "maximum defined data set" or "ceiling on the nature and number of data elements inherent to each standard," used to "ensure that health plans did not reject a transaction because it contained information they did not want." 65 Fed. Reg. at 50,322 (2000).

189 See 45 C.F.R. § 162.103.

190 See id.

191 See 45 C.F.R. § 162, Subparts K-R. The rule omits standards for first report of injury and claims attachments, to be addressed by separate rules. New and modified standards may be proposed and adopted pursuant to 45 C.F.R. §§ 160.104, 162.910. The transaction standards obviously do not apply to those electronic transactions for which standards are not specified in the rule (including, presumably, the two ignored "covered" transactions). 65 Fed. Reg. at 50,317.

192 The guides may be downloaded from the DHHS website, available at <http://aspe.hhs.gov/admsimp/>, or obtained as provided in 45 C.F.R. § 162.920(a).

193 The new code sets are as follows: (1) Diseases, Injuries, Impairments, Other health problems and their manifestations and Causes of injury, disease, impairment, or other health problems -- International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2 (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by DHHS; (2) Procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals (Prevention, Diagnosis, Treatment, Management)-- International Classification of Diseases, 9th Edition, Clinical Modification, Volume 3 Procedures (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by DHHS; (3) Drugs and Biologies -- National Drug Codes (NDC), as maintained and distributed by DHHS in collaboration with drug manufacturers; (4) Dental Services -- Code on Dental Procedures and Nomenclature, as maintained and distributed by the American Dental Association; (5) Physician services and other health care services, including, but not limited to: Physician services; Physical and occupational therapy services; Radiologic procedures; Clinical laboratory tests; Other medical diagnostic procedures; Hearing and vision services; Transportation services including ambulance -- Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by DHHS, and Current Procedural Terminology, Fourth Edition (CPT-4), as maintained and distributed by the American Medical Association; and (6) All other substances, equipment, supplies, or other items used in health care services, including, but not limited to Medical supplies; Orthotic and prosthetic devices; and Durable medical equipment -- The Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by DHHS.
furnished (medical services) or a transaction is initiated. Exceptions are made for the following: paper transactions; nursing home fixed indemnity policies; transmission of data by direct data entry (excepted only from format requirements); certain "atypical" services related to covered transactions; certain nonstandard transactions involving health care clearinghouses; and transactions using standards undergoing official testing.

As with the privacy and security provisions, criticism of the transmission standards and code set rules continues. The most predictable complaints focus on compliance costs, which could run as high as Y2K conversion. Others believe that the rules' compliance period is too short. Indeed, one recent online survey revealed that while all clearinghouses and 75% of vendors expected to timely achieve compliance, only half of payers expected to be compliant by October, 2002.

Nevertheless, compliance with transaction and code set standards will greatly ease claims and payment administration and reduce related costs over time. These rules will therefore likely facilitate compliance with the privacy and security standards. Accordingly, covered entities have an added incentive (apart from penalty provisions) to achieve compliance with these rules. If a covered entity is currently under an EDI contract with an outside vendor, it must ascertain whether

---

194 See 45 C.F.R. § 162.1000.
196 See id. at 50,319.
197 See 45 C.F.R. § 162.923. "Direct data entry" means "the direct entry of data (for example, using dumb terminals or web browsers) that it immediately transmitted into a health plan's computer." Id. § 162.103. This definition appears to include "certain transmission modes" used for data entry directly into systems within a health plan, such as "direct data entry" using dumb terminals or computer browser screens, as well as telephone voice response and "faxback" systems. See 65 Fed. Reg. at 50,315 (2000).
198 Relying on its definition of "health services" in 45 C.F.R. section 160.103, DHHS wrote the following:
[services that are not health care services or supplies under this definition are not required to be claimed using the standard transactions. Thus, claims for non-emergency transportation or carpentry services for housing services, if submitted, would not be required to be conducted as standard transactions. . . . Those atypical services that meet the definition of health care, however, must be billed using the standard if they are to be submitted electronically.] 65 Fed. Reg. at 50,316.
199 See 45 C.F.R. §§ 162.923(c), 162.930. The rule clarifies that covered transactions with health care clearinghouses generally must be standard; however, it also notes that "the statute permits a covered entity to submit nonstandard communications to a health care clearinghouse for processing into standard transactions and transmission by the health care clearinghouse as well as receive standard transactions through the health care clearinghouse." 65 Fed. Reg. at 50316.
200 See 45 C.F.R. § 162.940.
necessary software upgrades and training are included in the current contract.203 If not covered by contract, the entity must acquire the technology applications needed to (1) eliminate local medical procedure and terminology codes previously required by plans and state agencies, (2) upgrade software systems to handle standard formats or contracting with clearinghouse to convert standard data to current format, and (3) complete staff training.204

IV. CONCLUSION

Although some HIPAA "administrative simplification" rules have yet to be issued, or have been issued only in proposed form, it is evident from the breadth of existing rules that health care entities must quickly move to discover if, and to what extent, they are covered by the rules. Covered entities may expect to expend significant organizational resources to achieve HIPAA compliance. However, after consulting with legal and other professional counsel, covered entities may avoid undue compliance pressure by identifying HIPAA-related deficiencies and taking early corrective action.

203 See supra note 191.
204 See Waller, supra note 15, at 722; see also supra note 191.