

C. Transition to the Final Rule

The proposed rule included definitions for a number of terms that have now already been promulgated as part of the Transactions Rule or the Privacy Rule. Comments related to the definitions of “code set,” “health care clearinghouse,” “health plan,” “health care provider,” “small health plan,” “standard” and “transaction,” are addressed in the Transactions Rule at 65 FR 50319 through 50320. Comments concerning the definition of “individually identifiable health information” are discussed below, but are also addressed in the Privacy Rule at 65 FR 82611 through 82613. In addition, a few terms were redefined in the final Standards for Privacy of Individually Identifiable Health Information (67 FR 53182), issued on August 14, 2002 (Privacy Modifications). Certain terms that were defined in the proposed rule are not used in the final rule because they are no longer necessary. Other terms defined in the proposed rule are defined within the explanation of the standards in the final rule and are discussed in the preamble discussions in § 164.308 through § 164.312.

Definitions of terms relevant to the security standards now appear in the regulations text provisions as indicated below:

§ 160.103: Definitions of the following terms relevant to this rule appear in § 160.103: “business associate,” “covered entity,” “disclosure,” “electronic media,” “electronic protected health information,” “health care,” “health care clearinghouse,” “health care provider,” “health information,” “health plan,” “individual,” “individually identifiable health information,” “implementation specification,” “organized health care arrangement,” “protected health information,” “standard,” “use,” and “workforce.” These terms were discussed in connection with the Transaction and Privacy Rules and with the exception of the terms “covered entity” “disclosure” “electronic protected health information,” “health information,” “individual,” “organized health care arrangement,” “protected health information,” and “use,” we will not discuss them in this document. We note that the definition of those terms are not changed in the final rule.

§ 162.103: We have moved the definition of “electronic media” at § 162.103 to § 160.103 and have modified it to clarify that the term includes storage of information. The term “electronic media” is used in the definition of “protected health

information.” Both the privacy and security standards apply to information “at rest” as well as to information being transmitted.

We note that we have deleted the reference to § 162.103 in paragraph (1)(ii) of the definition of “protected health information,” since both definitions, “electronic media” and “protected health information,” have been moved to this section. Also, it is unnecessary, because the definitions of § 160.103 apply to all of the rule in parts 160, 162, and 164.

We have also clarified that the physical movement of electronic media from place to place is not limited to magnetic tape, disk, or compact disk. This clarification removes a restriction as to what is considered to be physical electronic media, thereby allowing for future technological innovation. We further clarified that transmission of information not in electronic form before the transmission, for example, paper or voice, is not covered by this definition.

§ 164.103: The following term “plan sponsor” now appears in the new § 164.103, which consists of definitions of terms common to both subpart C and subpart E (the privacy standards). This definition was moved, without substantive change, from § 164.501 and has the meaning given to it in that section, and comments relating to this definition are discussed in connection with that section in the Privacy Rule at 65 FR 82607, 82611 through 82613, 82618 through 82622, and 82629.

§ 164.304: Definitions specifically applicable to the Security Rule appear in § 164.304, and these are discussed below. These definitions are from, or derived from, currently accepted definitions in industry publications, such as, the International Organization for Standards (ISO) 7498–2 and the American Society for Testing and Materials (ASTM) E1762–95.

The following terms in § 164.304 are taken from the proposed rule text or the glossary in Addendum 2 of the proposed rule (63 FR 43271), were not commented on, and/or are unchanged or have only minor technical changes for purposes of clarification and are not discussed below: “access,” “authentication,” “availability,” “confidentiality,” “encryption,” “password,” and “security.”

§ 164.314: Four terms were defined in § 164.504(a) of the Privacy Rule (“common control,” “common ownership,” “health care component,” and “hybrid entity”). Because these terms apply to both security and privacy, their definitions have been moved to § 164.103 without change.

Those terms are discussed in the Privacy Rule at 65 FR 82502 through 82503 and at 67 FR 53203 through 53207.

1. Covered Entity (§ 160.103)

Comment: One commenter asked if transcription services were covered entities. The question arose because transcription is often the first electronic or printed source of clinical information. Concern was expressed about the application of physical safeguard standards to the transcribers working for transcription companies or health care providers, either as employees or as independent contractors.

Another commenter expressed concern that scalability was limited to only small providers. The commenter explained that Third Party Administrators (TPAs) allow claim processors to work at home. Some TPAs have noted that it would be impossible to comply with the security standards for home-based claims processors.

Response: A covered entity’s responsibility to implement security standards extends to the members of its workforce, whether they work at home or on-site. Because a covered entity is responsible for ensuring the security of the information in its care, the covered entity must include “at home” functions in its security process. While an independent transcription company or a TPA may not be covered entities, they will be a business associate of the covered entity because their activities fall under paragraph (1)(i)(a) of the definition of that term. For business associate provisions see proposed preamble section III.E.8. and § 164.308(b)(1) and § 164.314(c) of this final rule.

2. Health Care and Medical Care (§ 160.103)

Comment: One commenter asked whether “medical care,” which is defined in the proposed rule, and “health care,” which is not, are synonymous.

Response: The term “medical care,” as used in the proposed rule (63 FR 43242), was intended to be synonymous with “health care.” The term “medical care” is not included in this final rule. It is, however, included in the definition of “health plan,” where its meaning is not synonymous with “health care.” For a full discussion of this issue and its resolution, see the Privacy Rule (65 FR 82578).