

### 3. Health Information and Individually Identifiable Health Information 160.103)

We note that the definitions of “health information” and “individually identifiable health information” remain unchanged from those published in the Transactions and Privacy Rules.

a. *Comment:* A number of commenters asked that the definition of “health information” be expanded to include information collected by additional entities. Several commenters wanted the definition to include health information collected, maintained, or transmitted by any entity, and one commenter suggested the inclusion of aggregated information not identifiable to an individual. Several commenters asked that eligibility information be excluded from the definition of information. Several commenters wanted the definition broadened to include demographics.

*Response:* Our definition of health information is taken from the definition in section 1171(4) of the Act, which provides that health information relates to the health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual. The statutory definition also specifies the entities by which health information is created or received. We note that, because “individually identifiable health information” is a subset of “health information” and by statute includes demographic information, “health information” necessarily includes demographic information. We think this is clear as a matter of statutory construction and does not require further regulatory change.

b. *Comment:* Several commenters asked that we clarify the difference between “health information” and “individually identifiable” and “health information pertaining to an individual” as used in the August 12, 1998 proposed rule (63 FR 43242). Additionally, commenters asked that we be more consistent in the use of these terms and recommended use of the term “individually identifiable health information.”

Two commenters stated that it is important to distinguish between “health information pertaining to an individual” and “individually identifiable health information,” as in reporting statistics at various levels there will always be a need to bring forth information pertaining to an individual.

One commenter recommended that the standards apply only to individually identifiable health information. Another

stated that in § 142.306(b) of the proposed rule, “health information pertaining to an individual” should be changed to “individually identifiable health information,” as nonidentifiable information can be used for utilization review and other purposes. As written, the regulation text could limit the ability to use data, for example, from a clearinghouse for compliance monitoring.

*Response:* In general, we agree with these commenters, and note that these comments are largely mooted by the decision, reflected in § 164.306 below and discussed in section III.D.1. of this final rule, to cover only electronic protected health information in this final rule.

c. *Comment:* Several commenters stated that the definition of “individually identifiable health information” is not in the regulations and should be added.

*Response:* We note that the definition of “individually identifiable health information” appears at § 160.103, which applies to this final rule.

### 4. Protected Health Information (§ 160.103)

This term is moved from § 164.501 to § 160.103 because it applies to both subparts C (security) and E (privacy). See 67 FR 53192 through 531936 regarding the definition of “protected health information.”

Also, the term “electronic media” is included in paragraphs (1)(i) and (ii) of the definition of “protected health information,” as specified in this section.

In addition, we added the definitions of “covered functions,” “plan sponsor,” and “Required by law” to § 164.103.

### 5. Breach (§ 164.304)

*Comment:* One commenter asked that “breach” be defined.

*Response:* The term “breach” has been deleted and therefore not defined. Instead, we define the term “security incident,” which better describes the types of situations we were referring to as breaches.

### 6. Facility (§ 164.304)

This new term has been added as a result of changing the name of the “physical access control” standard to “facility access control.” This change was made based on comments indicating that the original term was not descriptive. We have defined the term “facility” as the physical premises and interior and exterior of a building.

### 7. Security Incident (§ 164.304)

*Comment:* We received comments asking that this term be defined.

*Response:* This final rule defines “Security incident” in § 164.304 as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”

### 8. System (§ 164.304)

*Comment:* One commenter asked that “system” be defined.

*Response:* This final rule defines “system,” in the context of an information system, in § 164.304 as “an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.”

### 9. Workstation (§ 164.304)

*Comment:* One commenter expressed concern that the use of the term “workstation” implied limited applicability to fixed devices (such as terminals), excluding laptops and other portable devices.

*Response:* We have added a definition of the term “workstation” to clarify that portable devices are also included. This final rule defines workstation as “an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.”

### 10. Definitions Not Adopted

Several definitions in the proposed regulations text and glossary are not adopted as definitions in the final rule: “participant,” “contingency plan,” “risk,” “role-based access control,” and “user-based access control.” The terms “participant,” “role-based access control,” and “user-based access control” are not used in this final rule and thus are not defined. “Risk” is not defined as its meaning is generally understood. While we do not define the term, we address “contingency plan” as a standard in § 164.308(a)(7) below.

a. *Comment:* We received comments requesting that we define the following terms: “token” and “documentation.”

*Response:* These terms were defined in Addendum 2 of the proposed rule. In this final rule, we do not adopt a definition for “token” because it is not used in the final rule. “Documentation” is discussed in § 164.316 below.

b. *Comment:* We received several comments that “small” and “rural” should be defined as those terms apply