breaches under this subpart, and therefore, covered entities and business associates need not provide breach notification in all cases of impermissible uses and disclosures. We also note that the HIPAA Security Rule provides for administrative, physical, and technical safeguards and organizational requirements for electronic protected health information, but does not govern uses and disclosures of protected health information. Accordingly, a violation of the Security Rule does not itself constitute a potential breach under this subpart, although such a violation may lead to a use or disclosure of protected health information that is not permitted under the Privacy Rule and thus, may potentially be a breach under this subpart.

The Act does not define the terms ''acquisition'' and ''access.'' Several commenters asked that we define or identify the differences between acquisition, access, use, and disclosure of protected health information, for purposes of the definition of ''breach.'' We interpret ''acquisition'' and ''access'' to information based on their plain meanings and believe that both terms are encompassed within the current definitions of ''use'' and ''disclosure'' in the HIPAA Rules. Accordingly, we have not added separate definitions for these terms. We have retained the statutory terms in the regulation in order to maintain consistency with the statute. In addition, we note that while the HIPAA Security Rule at § 164.304 includes a definition of the term ''access,'' such definition is limited to the ability to use ''system resources'' and not to access to information more generally and thus, we have revised that definition to make clear that it does not apply for purposes of these breach notification rules.

For an acquisition, access, use, or disclosure of protected health information to constitute a breach, it must constitute a violation of the Privacy Rule. Therefore, one of the first steps in determining whether notification is necessary under this subpart is to determine whether a use or disclosure violates the Privacy Rule. We note that uses or disclosures that impermissibly involve more than the minimum necessary information, in violation of §§ 164.502(b) and 164.514(d), may qualify as breaches under this subpart. In contrast, a use or disclosure of protected health information that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule pursuant to 45 CFR 164.502(a)(1)(iii) and, therefore, would not qualify as a potential breach. Finally, violations of administrative requirements, such as a lack of reasonable safeguards or a lack of training, do not themselves qualify as potential breaches under this subpart (although such violations certainly may lead to impermissible uses or disclosures that qualify as breaches).

Compromises the Security or Privacy of Protected Health Information

The Act and regulation next limit the definition of ''breach'' to a use or disclosure that ''compromises the security or privacy'' of the protected health information. Accordingly, once it is established that a use or disclosure violates the Privacy Rule, the covered entity must determine whether the violation compromises the security or privacy of the protected health information.

For the purposes of the definition of ''breach,'' many commenters suggested that we add a harm threshold such that an unauthorized use or disclosure of protected health information is considered a breach only if the use or disclosure poses some harm to the individual. These commenters noted that the ''compromises the security or privacy'' language in section 13400(1)(A) of the Act contemplates that covered entities will perform some type of risk assessment to determine if there is a risk of harm to the individual, and therefore, if a breach has occurred. Commenters urged that the addition of a harm threshold to the definition would also align this regulation with many State breach notification laws that require entities to reach similar harm thresholds before providing notification. Finally, some commenters noted that failure to include a harm threshold for requiring breach notification may diminish the impact of notifications received by individuals, as individuals may be flooded with notifications for breaches that pose no threat to the security or privacy of their protected health information or, alternatively, may cause unwarranted panic in individuals, and the expenditure of undue costs and other resources by individuals in remedial action.

We agree that the statutory language encompasses a harm threshold and have clarified in paragraph (1) of the definition that ''compromises the security or privacy of the protected health information'' means ''poses a significant risk of financial, reputational, or other harm to the individual.'' This ensures better consistency and alignment with State breach notification laws, as well as existing obligations on Federal agencies (some of which also must comply with these rules as HIPAA covered entities) pursuant to OMB Memorandum M–07–16 to have in place breach notification policies for personally identifiable information that take into account the likely risk of harm caused by a breach in determining whether breach notification is required. Thus, to determine if an impermissible use or disclosure of protected health information constitutes a breach, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In performing the risk assessment, covered entities and business associates may need to consider a number or combination of factors, some of which are described below.[7]

Covered entities and business associates should consider who impermissibly used or to whom the information was impermissibly disclosed when evaluating the risk of harm to individuals. If, for example, protected health information is impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules or to a Federal agency that is obligated to comply with the Privacy Act of 1974 (5 U.S.C. 552a) and the Federal Information Security Management Act of 2002 (44 U.S.C. 3541 *et seq.*), there may be less risk of harm to the individual, since the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. In contrast, if protected health information is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater.

We expect that there may be circumstances where a covered entity takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such steps eliminate or reduce the risk of harm to the individual to a less than ''significant risk,'' then we interpret that the security and privacy of the

[7] Covered entities may also wish to review OMB Memorandum M–07–16 for examples of the types of factors that may need to be taken into account in determining whether an impermissible use or disclosure presents a significant risk of harm to the individual.

information has not been compromised and, therefore, no breach has occurred.

In addition, there may be circumstances where impermissibly disclosed protected health information is returned prior to it being accessed for an improper purpose. For example, if a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, such a breach may not pose a significant risk of harm to the individuals whose information was on the laptop. Note, however, that if a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.

In performing a risk assessment, covered entities and business associates should also consider the type and amount of protected health information involved in the impermissible use or disclosure. If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach. For example, if a covered entity improperly discloses protected health information that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual. In contrast, if the information indicates the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program [8]), or if the protected health information includes information that increases the risk of identity theft (such as a social security number, account number, or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information. The risk assessment should be fact specific, and the covered entity or business associate should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of the risk of reputational harm—especially in light of fears about employment discrimination.

We also address impermissible uses and disclosures involving limited data sets (as the term is used at 45 CFR 164.514(e) of the Privacy Rule), in paragraph (1) of the definition of ''breach'' at § 164.402 of the interim final rule. In the RFI discussed above, we asked for public comment on whether limited data sets should be considered unusable, unreadable, or indecipherable and included as a methodology in the guidance. A limited data set is created by removing the 16 direct identifiers listed in § 164.514(e)(2) from the protected health information.[9] These direct identifiers include the name, address, social security number, and account number of an individual or the individual's relative, employer, or household member. When these 16 direct identifiers are removed from the protected health information, the information is not completely de-identified pursuant to 45 CFR 164.514(b). In particular, the elements of dates, such as dates of birth, and zip codes, are allowed to remain within the limited data set, which increase the potential for re-identification of the information. Because there is a risk of re-identification of the information within a limited data set, the Privacy Rule treats this information as protected health information that may only be used or disclosed as permitted by the Privacy Rule.

Several commenters suggested that the limited data set should not be included in the guidance as a method to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required. These commenters cited concerns about the risk of re-identification of protected health information in a limited data set and noted that, as more data exists in electronic form and as more data becomes public, it will be easier to combine these various sources to re-establish the identity of the individual. Furthermore, due to the risk of re-identification, these commenters stated that creating a limited data set was not comparable to encrypting information, and therefore, should not be included as a method to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

The majority of commenters, however, did support the inclusion of the limited data set in the guidance. These commenters stated that it would be impractical to require covered entities and business associates to notify individuals of a breach of information within a limited data set because, by definition, such information excludes the very identifiers that would enable covered entities and business associates, without undue burden, to identify the affected individuals and comply with the breach notification requirements. Additionally, these commenters cited contractual concerns regarding the data use agreement, which prohibits the recipient of a limited data set from re-identifying the information and therefore, may pose problems with complying with the notification requirements of section 13402(b) of the Act.

These commenters also noted that the decision to exclude the limited data set from the guidance, such that a breach of a limited data set would require breach notification, would reduce the likelihood that covered entities would continue to create and share limited data sets. This, in turn, would have a chilling effect on the research and public health communities, which rely on receiving information from covered entities in limited data set form.

Finally, commenters noted that the removal of the 16 direct identifiers in the limited data set presents a minimal risk of serious harm to the individual by limiting the possibility that the information could be used for an illicit purpose if breached. These commenters also suggested that the inclusion of the limited data set in the guidance would align with most state breach notification laws, which, as a general matter, only require notification when certain identifiers are exposed and when there is a likelihood that the breach will result in harm to the individual.

We also asked commenters if they believed that the removal of an individual's date of birth or zip code, in addition to the 16 direct identifiers in 45 CFR 164.514(e)(2), would reduce the risk of re-identification of the information such that it could be included in the guidance. Several commenters responded to this question. While some stated that the removal of these data elements would render the

[8] Note that an impermissible disclosure that indicates that an individual has received services from a substance abuse treatment program may also constitute a violation of 42 U.S.C. 290dd–2 and the implementing regulations at 42 CFR part 2. These provisions require the confidentiality of substance abuse patient records.

[9] A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) Names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) Web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.