ACCOUNTABILITY

This is one of a series of companion documents to *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (Privacy and Security Framework). This guidance document provides information regarding the HIPAA Privacy Rule as it relates to the Accountability Principle in the Privacy and Security Framework.

ACCOUNTABILITY PRINCIPLE: The Principles in the Privacy and Security Framework should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

ACCOUNTABILITY AND THE HIPAA PRIVACY RULE

The Accountability Principle in the Privacy and Security Framework emphasizes that compliance with, and appropriate mechanisms to report and mitigate non-compliance with, the Principles are important to building trust in the electronic exchange of individually identifiable health information. The Privacy Rule provides the foundation for accountability within an electronic health information exchange environment by requiring covered entities that exchange protected health information (PHI), whether on paper or electronically, to comply with its administrative requirements and extend such obligations to their business associates. The Privacy Rule also promotes accountability by establishing mechanisms for addressing potential non-compliance with privacy standards through a covered entity's voluntary compliance, a resolution agreement and corrective action plan, or the imposition of civil money penalties, if necessary.

Administrative Requirements

The Privacy Rule's administrative requirements provide a management, accountability, and oversight structure for covered entities to ensure that proper safeguards and policies and procedures are in place for PHI. See 45 C.F.R. § 164.530. The Privacy Rule provides covered entities considerable flexibility, however, to develop and implement policies and procedures which are appropriate and scalable to their own environment. This flexibility allows covered entities that will be engaging in electronic health information exchange to or through a health information organization (HIO) to consider how best to comply with the Privacy Rule's administrative standards.

Workforce Training and Sanctions

The Privacy Rule requires a covered entity to have written policies and procedures as necessary to implement the privacy standards in the Rule and to train workforce members on those policies and procedures, as necessary and appropriate for the workforce members to perform their functions. See 45 C.F.R. § 164.530(b). A covered entity also must have and apply appropriate sanctions for workforce members who violate the Privacy Rule or the entity's own privacy policies and procedures. See 45 C.F.R. § 164.530(e).

Covered entities either will need to write new privacy policies and procedures or adapt their existing policies and procedures to address the changes in their business practices needed to accommodate electronic exchanges of PHI to or through a HIO. Workforce members, whose functions involve the electronic exchange of PHI to or through a HIO, including those workforce members responsible for monitoring and overseeing the entity's participation in an electronic health information exchange, should receive training on these new or changed policies and procedures. A covered entity engaging in the electronic exchange of PHI to or through a HIO also should review and amend as necessary its policies and procedures for sanctioning workforce members who fail to comply with the entity's privacy policies and procedures or the requirements of the Privacy Rule. As the covered entity's privacy practices may change to accommodate electronic exchanges of information to or through a HIO, the entity's sanction policies may likewise need to address changes in responsibility for accessing, using, and disclosing PHI, the types of noncompliance that may arise in an electronic environment, and the appropriate sanctions for such noncompliance. For example, electronic access privileges may need to be suspended or even revoked for workforce members found to be abusing such privileges.

Complaint Process

The Privacy Rule requires a covered entity to develop and implement procedures which allow individuals to make complaints about its compliance with the Privacy Rule, as well as its own privacy policies and procedures. See 45 C.F.R. § 164.530(d). Through this complaint mechanism, covered entities can learn of and address the problems and concerns of individuals with the entity's privacy practices, including concerns or problems involving the electronic exchange of PHI to or through a HIO. The covered entity's notice of privacy practices should inform individuals of how to file a complaint and provide appropriate contact information. See 45 C.F.R. § 164.520(b)(1)(vi)-(vii).

Mitigation

Under the Privacy Rule, at 45 C.F.R. § 164.530(f), a covered entity must mitigate, to the extent practicable, any harmful effects that are known to the covered entity and that result from a use or disclosure of PHI in violation of its own privacy policies and procedures or the Privacy Rule by the covered entity or its business associates. Thus, mitigation is required, where practicable, for known harmful effects caused by the covered entity's own workforce misusing or disclosing electronic PHI or by such misuse or wrongful disclosure by a HIO that is a business associate

of the covered entity. While appropriate steps to mitigate harm caused by an improper use or disclosure in an electronic environment will vary based on a totality of the circumstances, some mitigation steps to consider would be:

- Identifying the cause of the violation and amending privacy policies and technical procedures, as necessary, to assure it does not happen again;
- Contacting the network administrator, as well as other potentially affected entities, to try to retrieve or otherwise limit the further distribution of improperly disclosed information;
- Notifying the individual of the violation if the individual needs to take self-protective measures to ameliorate or avoid the harm, as in the case of potential identify theft.

Liability for Violations of the HIPAA Privacy Rule in an Electronic Health Information Exchange Environment

Liability for civil money penalties arising from violations of the Privacy Rule continues to rest exclusively on covered entities, even in an electronic health information exchange environment. Thus, covered entities that participate in or exchange PHI to or through a HIO are responsible for their own non-compliance with the Privacy Rule, as well as that of their workforce. HIOs that are not otherwise covered entities in their own right are not directly liable for noncompliance with the Privacy Rule. However, where a business associate agreement exists between a covered entity and a HIO for the electronic exchange of PHI, the HIO will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by the business associate, and if unable to do so, to terminate the business associate relationship. Pursuant to its business associate agreement, the business associate is required to extend these contractual provisions to its agents or subcontractors, as well. See 45 C.F.R. §§ 164.502(e), 164.504(e). See also the parallel business associate requirements in the HIPAA Security Rule at 45 C.F.R. § 164.314(a).

Accountability and the Business Associate Agreement

The Privacy Rule requires business associate agreements to contain satisfactory assurances that a business associate will adequately safeguard PHI. Some of the satisfactory assurances by a HIO acting as a business associate would include, for example, that:

- the HIO will not use or disclose PHI except as allowed by the agreement;
- the HIO will implement reasonable and appropriate safeguards for PHI; and
- the HIO will report any uses or disclosures of PHI that violate the agreement to the covered entity.

Although the Privacy Rule requires business associates to self-report to the covered entity uses and disclosures of PHI that constitute a material breach or violation of the agreement, the covered entity may want to consider other means and methods to monitor the activities of the HIO and its compliance with its business associate obligations. Where, through the business associate self-reports or based on other substantial and credible evidence, the covered entity becomes aware of a pattern or practice by the HIO in material breach or violation of the agreement, the covered entity must attempt to cure the breach or end the violation by the HIO. If such attempts are unsuccessful, the Privacy Rule would require the covered entity to terminate its agreement with the HIO. In the event termination is not feasible, the covered entity must report the HIO's violation(s) to the Secretary of HHS through OCR.

FREQUENTLY ASKED QUESTIONS

Q1: What is a covered entity's liability under the HIPAA Privacy Rule for sharing data inappropriately to or through a health information organization (HIO) or other electronic health information exchange network?

A1: A covered entity that exchanges protected health information (PHI) to or through a HIO or otherwise participates in electronic health information exchange is responsible for its own non-compliance with the Privacy Rule, and for violations by its workforce. A covered entity is not directly liable for a violation of the Privacy Rule by a HIO acting as its business associate, if an appropriate business associate agreement is in place. Nor can a HIO as a business associate be held liable for civil money penalties arising from violations of the Privacy Rule. Rather, where a business associate agreement exists between a covered entity and a HIO for the electronic exchange of PHI, the HIO will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by the business associate, and if unable to do so, to terminate the business associate relationship. See 45 C.F.R. §§ 164.502(e), 164.504(e). Furthermore, a covered entity is not liable for a disclosure that is based on the non-compliance of another entity within the health information exchange, as long as the covered entity has complied with the Privacy Rule.

Q2: Does the HIPAA Privacy Rule require a covered entity to "police" a health information organization (HIO), which functions as its business associate?

A2: No. As with other business associates, the Privacy Rule would require that a covered entity enter into a relationship with a HIO in a way which anticipates and reasonably safeguards against the potential for inappropriate uses and disclosures, specifically through the use of a business associate agreement. The Privacy Rule also would require the covered entity to respond appropriately to complaints and evidence of violations, but it would not

otherwise require the covered entity to actively monitor or oversee the extent to which a HIO, acting as its business associate, abides by the privacy provisions of the agreement, or the means by which the HIO carries out its privacy safeguard obligations. See 45 C.F.R. §§ 164.502(e), 164.504(e).

Q3: How should a covered entity respond to any HIPAA Privacy Rule violation of a health information organization (HIO) acting as its business associate?

A3: The Privacy Rule establishes a series of steps a covered entity should take in response to any complaints or other evidence it receives that a HIO has violated its business associate agreement, which include the following:

- investigation of any complaint received, as well as of other information containing credible evidence of a violation;
- reasonable steps to cure/end any material breaches or violations it becomes aware of;
- termination of the agreement where attempts to cure a material breach are unsuccessful; and
- in the event termination of the agreement is not feasible, the report of violation(s) to the Secretary of HHS, through OCR. See 45 C.F.R. § 164.504(e).

Q4: Who is liable under the HIPAA Privacy Rule where multiple covered entities have signed on to a single business associate agreement and one member breaches the agreement?

A4: The Privacy Rule is flexible enough to allow multiple covered entities to exchange information with each other in an electronically networked environment upon entering into a single, multi-party business associate agreement. Regardless of the number of signatories, the obligations in a multi-party business associate agreement will be largely bi-directional. Covered entities will still be accountable for the actions of their workforce, as well as the contents and enforcement of its business associate agreement with the health information organization (HIO). See 45 C.F.R. §§ 164.530(b),(e) and 164.504(e). Covered entities will not be liable, however, for the violations of other participants in the HIO's health information exchange.