TRICARE

TMA Privacy Office Information Paper

Records Management◆FOIA◆DUAs◆HIPAA Compliance◆ADP Security◆Privacy Act◆System of Records◆PIAs

Documentation of Security Actions

HIPAA Security◆ November 2003

Standard Requirement

The Security Rule requires covered entities to "maintain the policies and procedures implemented to comply with the [Security Rule] in written (which may be electronic) form" and maintain a "written (which may be electronic) record" of any "action, activity or assessment" that is required by the standards and implementation specifications of the Rule.

This standard includes two parts. The first part requires covered entities to document in written format (paper or electronic) policies and procedures pertaining to the protection of electronic protected health information. When organizations develop and maintain their policies and procedures as part of an "oral tradition" only, they become vulnerable to several threats. Orally developed and transmitted policies tend to drift in response to local circumstances thus helping produce varying practice across the organization. In the absence of written rules, organizations inconsistently and incompletely train personnel and find consistent enforcement difficult or impossible. Maintaining policies and procedures in written format safeguards against these threats. The second part requires covered entities to document the results of implementing the policies and procedures when required by a standard or implementation specification. That would include risk analyses and risk management reports conducted as part of the security management process, security incident reports, all business associate contracts, designations of security officers, and so on. This serves several purposes. Examination of the records for patterns of activity can reveal threats and vulnerabilities, allowing the covered entity to take action to improve the security of protected health information. Because written records demonstrate compliance with policies and procedures, auditors and other surveyors often request to review them during inspections. And finally written records can demonstrate due diligence. Documentation must be "detailed enough to communicate the security measures taken and to facilitate [the] periodic evaluations" required by the security evaluation standard of the administrative safeguards. (Final Rule, p.8361)

Implementation Specifications

There are three required implementation specifications associated with the documentation standard:

Documentation of Security Actions

- Time limit
- Availability
- Updates