Documentation of HIPAA Security Implementation Standards

The HIPAA Privacy regulations required the adoption of formal policies and procedures. For the HIPAA Security Standards, the documentation is even more important. Clinical practices must assess their need to comply with an addressable or required standard, implement an alternative measure, or not implement any measure at all as long as the practice will still meet the security standard to which it applies. The rationale behind such decisions must be adequately documented.

To assist our insureds in this process, what follows is an example of documentation of a security decision. In this example, our fictitious practice, Dental Practice Group (DPG) has looked at an addressable implementation specification under the transmission security standard. The standard requires the practice to "implement technical security measures to guard against unauthorized access to EPHI transmitted over an electronic communications network."

DPG has looked at the addressable implementation specification of encryption. They assessed the situation and ultimately decided not to use encryption to address the security standard. Here is the documentation they used to back up their decision.

SAMPLE POLICY

Current State Assessment Criteria

To ensure:

1. That EPHI that is transmitted electronically is not vulnerable to interception; and

2. That DPG's policies and procedure address HIPAA security requirements.

Current State Security Assessment

Readily available network access to claims information by clearinghouses is a benefit to DPG as well as its business associates. It promotes good business relations and services as a cost-efficient tool that allows DPG's staff to access information more quickly and efficiently.

The following gaps in security have been observed:

- There is no organization-wide policy governing access to PHI by health care clearinghouses. Sometimes information is e-mailed to other organizations, other times the organizations are given access to the private network containing EPHI and claims information;
- E-mail transmissions of EPHI over the Internet to clearinghouses are not protected, and could be intercepted by unauthorized users.

Risk Assessment

The risk of interception of claims information by unauthorized users over an open network is high, and the consequences of such interception are substantial. E-mail transmissions may be intercepted, allowing others to gain access to EPHI. DPG has no way of knowing whether e-mail transmissions have been intercepted and access to EPHI has been acquired. Intercepted information substantially increases the risk of wrongful disclosure of patient health information. Improperly secured information can subject DPG to penalties, possible civil and/or criminal action, including imprisonment, and irreparable harm to its reputation.

Options and Consequences

Option #1 (Implementation Specification):
Encrypt all information made available to clearinghouses. Consequence: Information is protected it if is intercepted, but computer response time is slowed considerably as a result of each piece of information that needs to be encrypted.

Option #2 (Alternative)
Limit electronic communications involving EPHI to the existing Web link for each clearinghouse, which permits unencrypted information to flow only to that organization. Clearinghouses will be given authentication codes to ensure that they are entitled to access and receive information. Consequence: Unauthorized third parties will not have access to information if it is intercepted, and computer systems remain at optimum speed.

Decision

To comply with HIPAA and protect the security of EPHI, DPG must implement technical policies and procedures for electronic information system that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.

DPG has decided to adopt Option #2 as an alternative to the implementation specification in the HIPAA security regulations that suggests encryption as a method of access control. Option #2 establishes reasonable and appropriate measures and demonstrates the commitment of DPG to protect against unauthorized access to EPHI. This option allows access of EPHI only to those organizations that are authorized to receive it and allows DPG to meet its obligation to keep EPHI secure.

Encrypting the information as outlined in Option #1 is not reasonable or appropriate. The slowed computer time would inhibit DPG to operate at an effective level. Encryption outlined in Option #1 would provide a higher degree of protection from unauthorized access to EPHI, however, such instances of unauthorized access are unlikely to occur, and Option #1 would therefore be excessive. The small likelihood of unauthorized access would not justify the negative business effects associated with encryption.