



Security Overview

SOS Online provides various levels of security related to accessing Electronic Protected Health Information (EPHI) which is the responsibility of a HIPAA covered entity.

Access Security

Data access policies and procedures focus on ensuring that users only access data for which they are appropriately authorized. Remote access to EPHI should only be granted to authorized users based on their role within the organization and their need for access to EPHI.

Storage Security

Storage policies and procedures address the security requirements for media and devices which contain EPHI and are moved beyond the covered entity's physical control. Such media and devices include laptops, hard drives, backup media, USB flash drives and any other data storage item which could potentially be removed from the organization's facilities.

Transmission Security

Transmission policies focus on ensuring the integrity and safety of EPHI sent over networks, and include both the direct exchange of data (for example, in trading partner relationships) and the provisioning of remote access to applications hosted by the organization (such as a provider's home access to ePrescribing systems or "web mail" in organizations where EPHI might be included in internal communications).