

ONC Takes On EHR Privacy and Security

✘ The sensitivity of health records and the need to defend against vulnerabilities in public access is nothing new, but as health IT becomes more and more ubiquitous and large-scale data breaches a common occurrence, privacy and security are increasingly top of mind.

While many hospital systems and physician practices have focused on digitizing their data, the Office of the National Coordinator for Health IT (ONC) has been ha

✘ The sensitivity of health records and the need to defend against vulnerabilities in public access is nothing new, but as health IT becomes more and more ubiquitous and large-scale data breaches a common occurrence, privacy and security are increasingly top of mind.

While many hospital systems and physician practices have focused on digitizing their data, the Office of the National Coordinator for Health IT (ONC) has been hard at work defining and updating the guidelines for privacy protection that are fast becoming industry standards.

At the start of the New Year, for example, the ONC published its guidelines on Safety Assurance Factors for Electronic Health Record (EHR) Resilience. The [SAFER Guides](#) recommend practices that optimize the safety and safe use of EHR's, including infrastructure guides mapping out contingency planning and clinical process guides on patient identification and clinician communication.

Most recently, the ONC put out a request for public comment by posing questions on their [blog](#) that seek input on one specific area of data privacy and how it might be addressed through policy changes.

The issue: What privacy concerns arise when a family member, friend or legal designee is given access to patient information through certified EHR technology? Some of the questions raised by the ONC include:

- Are there policy issues that need further resolution regarding personal representative access to view/download/transmit accounts?
- How do health-care providers confirm that an individual is, in fact, a personal representative?
- How are patients' friends and family provided with credentialed access to view/download/transmit accounts?
- Is this access "all or nothing," or are there more granular options? If the latter, how does this get accomplished?

With public feedback, the ONC's Health IT Policy Committee's Privacy and Security Tiger Team will be better adept at handling many critical questions around privacy and security. Those interested in keeping tabs on the ONC's latest thought leadership in this area are encouraged to follow their discussions here:

<http://www.healthit.gov/facas/calendar/2014/02/10/policy-privacy-security-tiger-team>

What should be the ONC's next top priority when it comes to privacy protection? Tweet @CNSICorp to let us know! Follow CNSI on [Twitter](#).