

Increased Patient Access under the 21st Century Cares Act: What it means for providers and why they need a HIPAA Compliance Check up Now

**For the Foundation for Orthopedic Research & Education
18th Annual Presentation of Current Solutions in Orthopedic Trauma
Saturday November 14, 2020**

Presented by:

Erin Smith Aebel, Esq.

Board Certified Health Lawyer

Trenam Law

101 E. Kennedy Blvd., Suite 2700,

Tampa, FL 33602

813-227-7455

eaebel@trenam.com



Overview

- 21 Century Cures Act
- HHS National Coordinator for Health Information Technology (ONC)
- Requirements for Health Care Providers effective April 5, 2021
- Exceptions for Providers
- Penalties
- HIPAA
- Overview
- Patient Right Of Access
- Security Rule Risk Assessment
- State law breach notification rules

21st Century Cares Act

- Bipartisan backed legislation signed into law by President Obama on 12/13/16.
- Likely to be supported and implemented by the Biden administration
- Aims to allow patients better access to their medical information
- Push to further promote value-based care
- Better interoperability of EHR

21st Century Cares Act

- Goal is to give patients safe, secure access to their health data so they can better manage their care.
- Patient access to their data helps them to make better and more informed decisions about their healthcare.
- Goal is to break down data silos and avoid fragmented healthcare.
- Legislation on the payer side too implemented by CMS (The presentation will focus only on patient access)

21st Century Cares Act

- Requires that health IT developers avoid existing or perceived anticompetitive information blocking that can prevent interoperability.
- Updates certification requirements for IT developers to ensure that they can communicate about health IT usability, user experience, interoperability, and security using screenshots and video.

21st Century Cares Act

- The ONC's final rule encourages allowing patients to obtain safe and secure access to their health information via smart phone apps.
- Health care providers, among other "actors" are prohibited from preventing patients with full access to their electronic health records.
- Information blocking includes:
 - Formally restricting access or use of electronic health information "EHI" through contracts or policies
 - Unnecessarily slowing or delaying access or otherwise limiting the timeliness of access to EHI
 - Charging an individual or their personal representative for electronic access to their EHI

21st Century Cares Act

- **Exceptions to information blocking**
- Preventing Harm Exception
- Reasonable belief the practice will substantially reduce a risk of harm
- Practice must be no broader than necessary

21st Century Cares Act

- **Exceptions to information blocking**
- Privacy Exception
- A provider should not have to provide access that is prohibited under a state or federal privacy law.
- ie. Psychotherapy notes

21st Century Cares Act

- **Exceptions to information blocking**
- Security Exception
- only if directly related to safeguarding the confidentiality, integrity and availability of EHI.
- tailored to specific security risks
- implemented in a consistent and non discriminatory manner.

21st Century Cares Act

- **Exceptions to information blocking**
- Infeasibility exception (Legitimate practical challenges)
- Health IT performance exception (IT may be offline temporarily)
- Content and Manner Exception.
- Fees exception
- Licensing Exception.

21st Century Cares Act

➤ Penalties

- The information blocking prohibition of the Cares Act applies to IT developers, health information exchanges (“HIE”) and health care providers.
- IT Developers and HIEs can be fined civil monetary penalties of 1m per violation for information blocking.
- Health care providers will not be subject to CMPs but will have the “appropriate disincentives”. (What does that mean?)

21st Century Cares Act

Practical Guidance: What do health care providers need to do and by when?

- The practical goal is for patients to have free and easy access to their electronic health records on their smart phones and other devices.
- Providers should work with their privacy and information security officers to understand what information blocking is and what exceptions they have to information blocking.
- Providers and their privacy and information security officers should work with their EHR vendors to determine how those vendors are working to allow patients more access under the 21st Century Cares Act and what steps they are taking to avoid information blocking. (These rules do not only apply to those IT providers who are part of the ONC's Health IT Certification Program.)
- Update policies and procedures and roll out training.
- review HIPAA and breach notification law and how this fits in with those laws.

HIPAA Review

- HIPAA Privacy Rule: Protects the privacy of protected health information (PHI) in any format- oral, written, electronic
- HIPAA Security Rule: Protects the security, integrity and availability of electronic protected health information (ePHI)
- Individuals have always had a statutory right of access to their health information in 45 CFR § 164.524.

HIPAA Review

Security Risk Assessment

- Individuals have a right to access their PHI in a designated record set. (Medical records and billing records and other info used by the provider to make decisions about the individual). Exclusion— psychotherapy notes.
- Personal representatives who have a right to make decisions for a patient have a right of access too.
- Patients may request access by a number of means including electronically. The provider may require that the individual request access in writing if they inform them of this requirement.
- Providers must take reasonable steps to verify that the individual has a right of access. Providers may not use unreasonable methods to verify right to access. (Request proof of identity in person when a patient is asking that the records be mailed to their home).
- Must provide access in electronic format if maintained electronically.
- Dovetails nicely with 21st Century Cares Act requirements.

HIPAA Breach Notification Requirements

- Only apply to a breach of unsecured ePHI
- Can the health information accessed by patients on their smart phones be encrypted to avoid a security breach and extensive notification requirements.
- Balance: Allow free electronic access without delay vs. electronic protections against breach, identity theft, hacking.
- Don't forget to review the breach notification laws in your home state. For example, the Florida Security Breach law at Fla. Stat. § 501.171.

Questions



Please feel free to contact the presenter with any questions.

Thank you!