

# Privacy and Security Problems and Plans

So many things and so little time to deal with them



## Hey Everybody!

*Hello! I'm...*

Donna Grindle

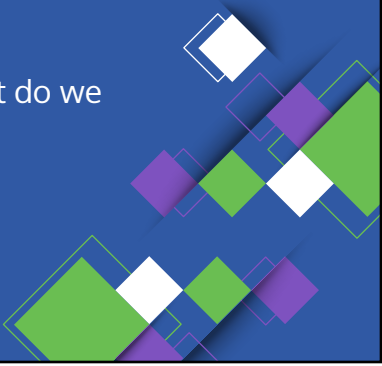
Kardon Founder

Help Me With HIPAA podcast

HHS 405d Task Group



# What will we be talking about?

- Patient access rights increased enforcement and Privacy Rule changes coming. Are you ready?
  - So many people want our data and systems. What do we do?
  - Information blocking? What the what?
- 



## Patient Right of Access Enforcement Privacy Rule Changes



*Our outreach and guidance hasn't worked. Therefore, we will be launching an enforcement initiative in 2019 to address patient rights to access of their records.*

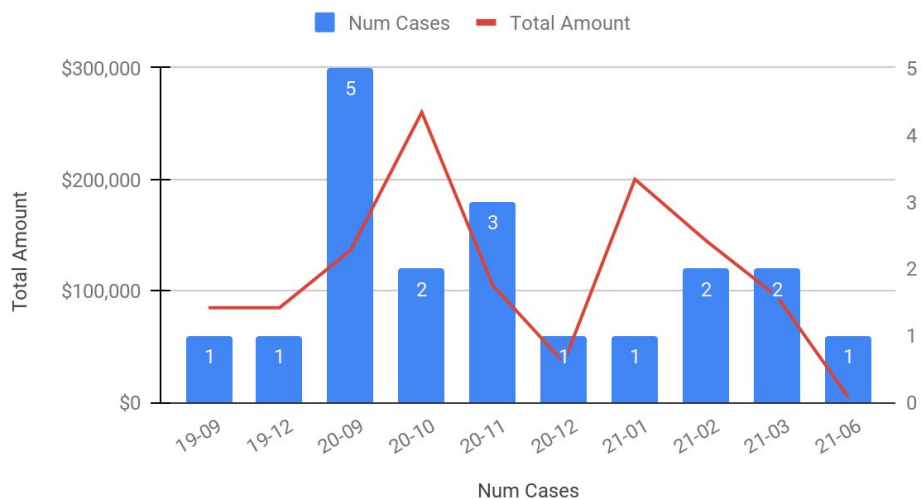
Roger Severino, Director OCR  
2019 HIPAA Summit Keynote

SLIDESMANIA.COM

KardonHQ.com



### Right of Access Enforcement Initiative



SLIDESMANIA.COM

KardonHQ.com

Settlements announced so far




# Two Types of Records Release

## Patient or Representative Requests


- Only disclosure **required** under HIPAA (few very minimal exceptions)
- Written requests but can be simply a note with signature
- Max 30 days to respond (possible 1-time 30 day extension)
- Limited fees can be charged
- Patient can opt out of secure exchange

## Authorized Disclosure

- Allowed but **not required**
  - Authorization must meet specific requirements
  - No timeframe required
  - States limit fees
  - Secured exchange required
- 



## Check fees, time frames, complete records

- **Fee** structure should match current requirements for direct to patient and third party options.
  - If possible supply in the **format** requested by patient or representative even if unsecured.
  - If stored electronically, it must be **provided electronically**.
  - **30 days** to supply **all requested records**.
    - Leaving out a single lab report can be a failure to provide complete records.
- 



## Length of time is biggest issues

Examples of delay length for 19 cases:

- 5 months
- 16 months
- 24 months
- 32 months

One completely refused to provide access to any parts of record until OCR stepped in.



## Frequently Learned Lessons

- Small Providers are NOT exempt
- Mental Health Providers are NOT exempt
- Valid third party directives must be met
- Complete records must be provided
- 30 days from request with one extension possible
- Only reasonable cost based fees



*It should not take a federal investigation before a HIPAA covered entity provides a parent with access to their child's medical records. Covered entities owe it to their patients to provide timely access to medical records.*

Robinsue Frohboese  
Acting OCR Director  
2021 Settlement Announcement



## Have you been scored?

ciitizen

### The Patient Record Scorecard

A deep analysis showing how medical record providers comply with the HIPAA Right of Access based on **patient requests**.

Scorecard reflects responses to patient requests for access starting on 2/10/19. Scoring is ongoing.

Check regularly <https://www.ciitizen.com/scorecard/>



# Ciitizen Star Rating System

★ **Not Compliant - Records Received**

Eventually got the records but not within guidelines

★★ **Compliant with Intervention**

Required Supervisor Intervention

★★★ **Compliant with Effort**

Multiple Phone Calls Required

★★★★ **Compliant Seamless Process**

Request Granted with Minimal Effort

★★★★★ **Compliant and Patient Focused**

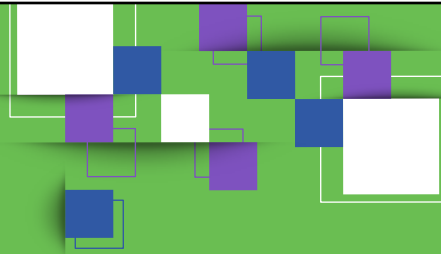
No Supervisor Intervention

Accepts External Request Forms

Sends Records in 5 Days or Less

No Fees

Records Sent to Patient Requested Destination



# Proposed Privacy Rule Changes



## Lots of changes may not happen

NPRM was huge and several items impact a lot of other things.

Expanding allowed disclosures is creating a lot of concern and pushback from privacy rights advocates.

Two things that may come through sooner than others.





# Notice of Privacy Practices Change

NPRM - Eliminate the requirement to obtain patient signature confirming receipt of NPP



## Notice of Privacy Practices Proposed Changes

- Eliminate the requirement to obtain patient signature confirming receipt of NPP
- Change specific wording of NPP to better explain to patients what their rights are under HIPAA and how to exercise those rights.
- Notes:
  - Have it **prominently** available on your website
  - Have current copies posted in public spaces that are easy to find
  - Provide written copies available whenever patient asks for one



# Patient Right of Access to PHI

- Shorten records request response time from 30 days to 15 calendar days with one 15 day extension
- Allow one provider to submit access request to another provider who is then **required** to send back electronic copies of PHI stored in an EHR
  - Currently providers are not **required** to disclose for treatment
  - This part relates directly to the information blocking requirements we will review next



## Cybersecurity Needs Attention Now!

# Cybersecurity Myths

A strong password makes me secure.

WiFi networks with passwords are safe to use.

Our IT people take care of all our security for us.

Antivirus software will block any cyber attacks.

If we have expensive security software we are secure.

We are HIPAA compliant that makes us secure.

Cyber criminals don't target SMBs.

We know how to recognize phishing emails.

Cyber criminals are our biggest concern.



SLIDESMANIA.COM

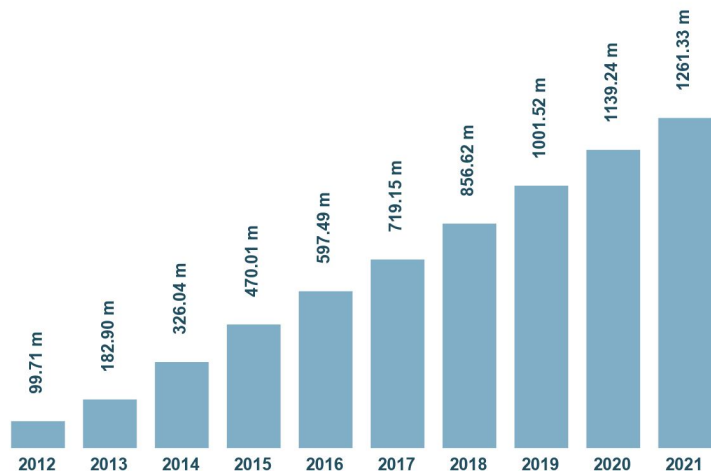
KardoniQ.com



We are currently tracking close to **1.3 Billion** different types of malware.

Total malware

**AVTEST**



Last update: August 29, 2021

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

SLIDESMANIA.COM

**94% of malware is delivered via email.**

**Inbox (6)**

Starred

Gifts

SHUTTERSTOCK.COM

Source: CSO Online

KardonHQ.com

**95% of  
cybersecurity  
breaches are a  
result of human  
error**



SHUTTERSTOCK.COM

Source: Cyberint

KardonHQ.com



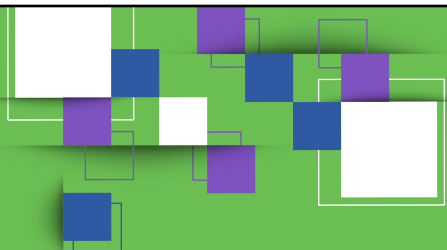
# 43% of cyber attacks target small businesses



# HIPAA is the floor

Do you only worry about securing the floor not the whole house?



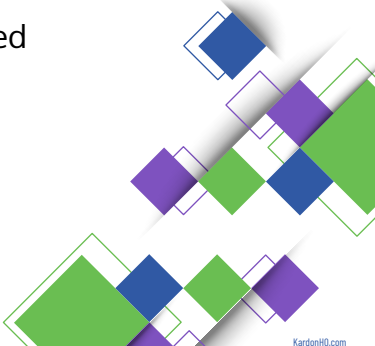


# Why do you care about Public Law No: 116-321?



## 2021 Amendment to HITECH

Require the Secretary of Health and Human Services to ***consider certain recognized security practices*** of covered entities and business associates ***when making certain determinations, and for other purposes.***



# Consider it how?

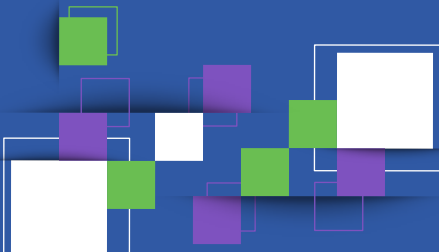
Possibly an early, favorable termination of a random audit.

May mitigate fines imposed for HIPAA violations defined in the original HITECH act.

May mitigate amount and terms in settlement agreements for resolving potential violations.



# You are NOT required to use Recognized Security Practices.



# There is no guarantee what the consideration in any case will be.

## What Are Recognized Security Practices?

The standards, guidelines, best practices, methodologies, procedures, and processes developed under the **NIST Framework for Improving Critical Infrastructure Cybersecurity**, the approaches promulgated under section **405(d) of the Cybersecurity Act of 2015** and other programs and processes that address cybersecurity that are developed, recognized, or promulgated through regulations under other statutory authorities.







**Ambassador for  
HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches

## NIST and 405(d)

- NIST Cybersecurity Framework
- Cybersecurity Act 2015 Section 405(d) Aligning Health Care Industry Security Approaches
- Other frameworks that meet requirements

# Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients

## 405(d)'s Cornerstone Publication

After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The Main Document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.

SLIDESMANIA.COM

KardoniHQ.com



## HICP 405D

HEALTH INDUSTRY CYBERSECURITY PRACTICES

### MAIN GUIDE

MANAGING THREATS & PROTECTING PATIENTS



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

## HICP 405D

HEALTH INDUSTRY CYBERSECURITY PRACTICES

### TECH VOLUME #1

PRACTICES FOR SMALL  
HEALTH CARE ORGANIZATIONS



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

## HICP 405D

HEALTH INDUSTRY CYBERSECURITY PRACTICES

### TECH VOLUME #2

PRACTICES FOR MEDIUM & LARGE  
HEALTH CARE ORGANIZATIONS



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

## HICP 405D

HEALTH INDUSTRY CYBERSECURITY PRACTICES

### RESOURCES & TEMPLATES



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

SLIDESMANIA.COM

KardoniHQ.com

## Technical 1 is for small organizations.



SLIDESMANIA.COM

40

KardoniHQ.com

## Technical 2 is for everyone else.

Using both Medium and Large practices.



SLIDESMANIA.COM



SLIDESMANIA.COM

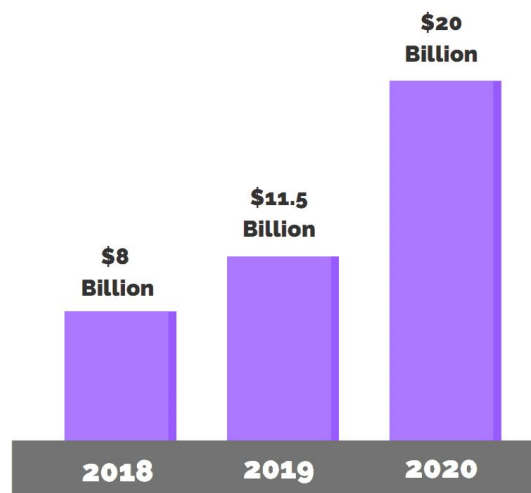
# Phishing

Sophisticated,  
targeted attacks by  
patient criminals.



KardoniQ.com

## Ransomware Is A Global Threat



\*Estimated global damage from ransomware. Source: Purplesec

2021 Likely to meet or exceed 2020 numbers

SLIDESMANIA.COM

KardoniQ.com



# Loss or Theft of Equipment or Data

SLIDESMANIA.COM

Kardoni0.com

**Internal,  
Accidental,  
or Intentional  
Data Loss**

SLIDESMANIA.COM


Kardoni0.com



# Attacks against Connected Medical Devices



## 10 Cybersecurity Practices

1. **Email** Protection Systems
  2. Endpoint Protection Systems
  3. Access Management
  4. Data Loss Prevention
  5. Asset Management
  6. Network Management
  7. Vulnerability Management
  8. **Incident Response**
  9. Medical Device Security
  10. Cybersecurity Policies
- 

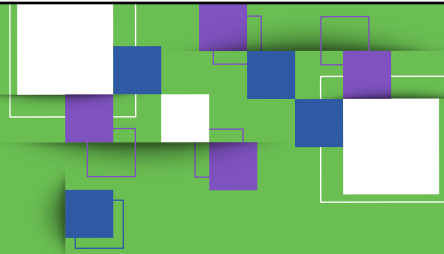


**Compliance  
is not  
security**

SLIDESMANIA.COM

**Security  
is not  
compliance**

KardoniQ.com



**21st Century Cures Act**

SLIDESMANIA.COM

KardoniQ.com



# Information Blocking

The **practice of information blocking** is blocking a patient's access to records.

The **Information Blocking Rule** defines what is considered blocking a patient's access to records.



# Information Blocking Practice


Interfering with access, exchange, or use of Electronic Health Information (EHI) *unless* there is a legal reason or one of the **8 specific exceptions** for doing so.



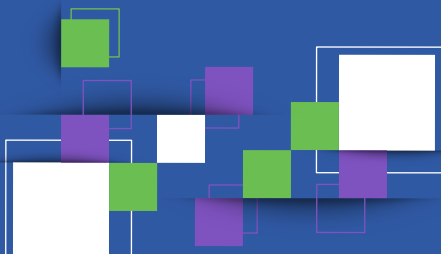


# Information Blocking Practice

There is **no requirement** under the information blocking regulations **to proactively** make available any EHI to patients or others ***who have not requested the EHI***. But, a delay in the release or availability of EHI ***in response to a request*** may still be considered information blocking.



Consider this as part of the shift from a *provider centered* system to a *patient centered* system.



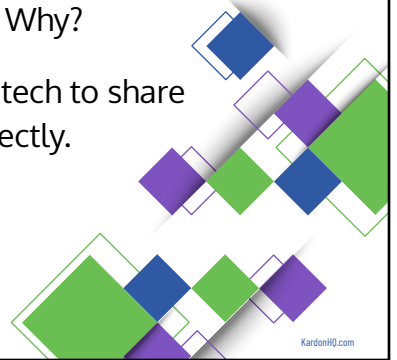
# Records Access



## Patient Centered

Today a patient is responsible for getting their records from each provider and being the courier between them. Why?

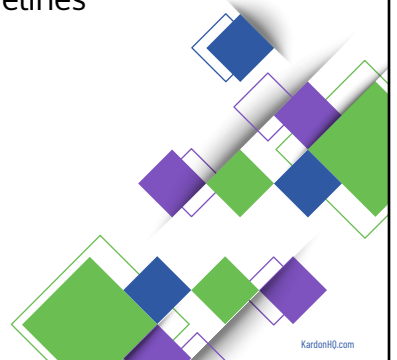
Providers have tech to share information directly.



## April 5th

## Effective Date


Only within these guidelines for now.





# Immediate Access Requests Only

There is **no requirement** under the information blocking regulations **to proactively** make available any EHI to patients or others ***who have not requested the EHI***. But, a delay in the release or availability of EHI ***in response to a request*** may still be considered information blocking.



SLIDESMANIA.COM

KardoniQ.com



**Must Only Address Patient  
Specific Requests For Now**

SLIDESMANIA.COM

KardoniQ.com

# “Actors”

Nope, not this kind  
of acting

SLIDESMANIA.COM

KardoniHQ.com

## “Actors” covered by rules



**Health Care  
Providers**



**Health Information Networks  
(HIN)/Health Information  
Exchanges (HIE)**



**Health IT Developer  
of Certified Health IT**

SLIDESMANIA.COM

KardoniHQ.com



# Electronic Health Information (EHI)

- Not the same as PHI Designated Record Set - YET
- Defined by ONC: United States Core Data for Interoperability (USCDI) v1
  - V2 in draft form mentioned in AHA letter
- In most basic definition, it means all the details about the patient's health that are stored within the EHR for now

## A SET OF DATA CLASSES TO SUPPORT NATIONWIDE INTEROPERABILITY

The USCDI Version 1 (USCDI v1) is proposed as a standard (§ 170.213). It reflects the same data classes referenced by the CCDS definition and includes new required data classes and data elements, noted below.

If adopted, health IT developers will need to update their certified health IT to support the USCDI for all certification criteria affected by this change.

### USCDI v1

#### Assessment and Plan of Treatment

#### Care Team Members

#### Clinical Notes \*NEW

- Consultation Note
- Discharge Summary Note
- History & Physical
- Imaging Narrative
- Laboratory Report Narrative
- Pathology Report Narrative
- Procedure Note
- Progress Note

#### Goals

- Patient Goals

#### Health Concerns

#### Immunizations

#### Laboratory

- Tests
- Values/Results

#### Medications

- Medications
- Medication Allergies

#### Patient Demographics

- First Name
- Last Name
- Previous Name
- Middle Name (including middle initial)
- Suffix
- Birth Sex
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Address \*NEW
- Phone Number \*NEW

#### Problems

#### Procedures

#### Provenance \*NEW

- Author
- Author Time Stamp
- Author Organization

#### Smoking Status

#### Unique Device Identifier(s) for a Patient's Implantable Device(s)

#### Vital Signs

- Diastolic Blood Pressure
- Systolic Blood Pressure
- Body Height
- Body Weight
- Heart Rate
- Respiratory rate
- Body Temperature
- Pulse oximetry
- Inhaled oxygen concentration
- Pediatric Vital Signs \*NEW
  - BMI percentile per age and sex for youth 2-20
  - Weight for age per length and sex
  - Occipital-frontal circumference for children < 3 years old



# 8 Exceptions: Actions Not Considered IB Practices

SLIDESMANIA.COM

KardoniQ.com

**No Blanket  
Exceptions**



KardoniQ.com

# Normal Policies Being Followed



KardonHQ.com



  
**PREVENTING  
HARM  
EXCEPTION**

  
**PRIVACY  
EXCEPTION**

  
**SECURITY  
EXCEPTION**

**EXCEPTIONS THAT INVOLVE  
not fulfilling requests to access,  
exchange, or use EHI**

  
**INFEASIBILITY  
EXCEPTION**

  
**HEALTH IT  
PERFORMANCE  
EXCEPTION**

**8**

**EXCEPTIONS TO THE  
INFORMATION  
BLOCKING  
PROVISION**

  
**LICENSING  
EXCEPTION**

  
**FEES  
EXCEPTION**

  
**CONTENT AND  
MANNER  
EXCEPTION**

**EXCEPTIONS THAT INVOLVE  
procedures for fulfilling requests  
to access, exchange, or use EHI**

## Enforcement



Actors that are subject to the information blocking regulations **may be investigated by the HHS Office of Inspector General** if they are the subject of a claim of information blocking.

## Different provider enforcement

**Developers and HIEs** - Civil monetary penalties up to \$1 million per violation.

**Providers** - Appropriate *disincentives* to be established by the Secretary.





OIG has stated they do not intend to penalize conduct occurring until *60 days after the final enforcement rules are effective.*

Rules have not been announced at this time.

# THANK YOU!



# HelpMeWithHIPAA.com

# KardonHQ.com

