Buckle Up Buttercup: HIPAA Changes Are Here

Bea Tolsdorf, Esq.
Samarria Dunson, J.D., CHC, CHPC
Continuing Education Disclosure

Samarria Dunson & Bea Tolsdorf, Balch & Bingham

1. I have no relevant financial relationships with any ACCME-defined commercial interest* to disclose.
2. I will not discuss off label use and/or investigational use in my presentation.
3. All Ascension planners, reviewers, and course directors have no relevant financial relationships with ACCME-defined commercial interests

*A commercial interest is any entity producing, marketing, re-selling, or distributed health care good and services consumed by, or used on, patients.

ASCENSION NURSING Center of Excellence
Information Blocking

New Rules for Access and Transmission of
Electronic Health Information

Presented by:
Bea Tolsdorf, Partner, Balch & Bingham LLP
Highlights for Discussion

• What is the new rule?
• What is required?
• Are there any exceptions to the rule?
• What are the penalties for non-compliance?
• What do you need to do to comply?
HOW DID WE GET HERE?

• Section 4004 of the 21st Century Cures Act
• 42 U.S.C.A § 300jj-52
• 45 C.F.R. §§ 171
• Concerns over practices that unreasonably limit the availability and use of “Electronic Health Information”
• Providers must not engage in practices that constitute Information Blocking.
• Related to HIPAA and state information laws
The New Rule – What is Information Blocking?

• Information Blocking is a business practice that is:
  1. Likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI AND
  2. If conducted by:
      • A health IT developer, exchange, or network that knows or should know that the practice will interfere, prevent or discourage access, exchange or use of EHI or
      • A healthcare provider that knows such practice is unreasonable and that it will burden the access, exchange or use of EHI

• Information Blocking doesn’t include a practice required by law, or those practices subject to an exception to the rule.
What is EHI?

• EHI stands for Electronic Protected Health Information.
• It does not include:
  • Psychotherapy notes
  • Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
EHI – Before October 6, 2022

- Patient demographics
- Vital signs
- Allergies and intolerances
- Medications
- Smoking status
- Immunizations
- Procedures
- Care team members

- Clinical notes
- Assessment and plan of treatment
- Goals
- Health concerns
- Laboratory
- Problems
- Unique Device Identifiers
- Provenance
The entire Designated Record Set under HIPAA.

HIPAA defines “Designated Record Set” as groups of records that are:

- Medical records and billing records for an individual maintained by or for health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used by or for a covered entity to make decisions about an individual.
WHO MUST COMPLY?

• Health Providers
  • “Hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center . . . renal dialysis facility, blood center, ambulatory surgical center . . . emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician . . . a practitioner . . . a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe . . . tribal organization, or urban Indian organization . . . a rural health clinic, a covered entity under section 256b of this title, . . . a therapist . . . and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.”

• Health Information Networks
• Health Information Exchanges
• ONC-Certified Health IT Developers
STANDARDS FOR COMPLIANCE

• Health care providers- knows such practice to be unreasonable and likely to interfere with access, exchange, or use of EHI.

• ONC-certified health IT developers, HINs, or HIEs- knows, or should know that such practice is likely to interfere with access, exchange, or use of EHI.
FULFILLING A REQUEST

• Must fulfill in any manner requested.

• If unable to fulfill in the requested manner
  • Work with requestor to develop alternative manner
  • If agreement cannot be reached, fulfill in the manner described in the final rule.
EXCEPTIONS

• For not fulfilling requests
  • Preventing harm
  • Privacy
  • Security
  • Infeasibility
  • Health IT performance

• For fulfilling requests with limitations
  • Content and manner
  • Fees
  • Licensing
PENALTIES

• Health care providers
  • Disincentives determined in future HHS rulemaking
  • Reports from CMS to MIPS

• Certified Health IT, HINs, and HIEs
  • CMPs up to $1M per violation
  • Separate enforcement from ONC
SCENARIOS

• Patient requests EHI from provider and provider takes 10 months to fulfill request when it was capable of doing so sooner.

• Individual requests EHI returned by email and provider mails physical copies to individual instead.

• Patient requests copies of treatment notes from provider. Provider has a policy of denying requests for notes that are handwritten by physician, and only releasing those that have been typed and stored in the provider database.
TAKEAWAYS

• Update policies regarding record requests for compliance
• Efficiently release EHI upon request in a way that isn’t “information blocking”
• May deny or delay fulfilling the request if required to do so by law or if an exception applies
• EHI definition is limited now, but will expand to the designated record set on October 6, 2022
• Fulfill the request in the manner requested unless it is impossible to do so
2021 HITECH Amendment

HIPAA
Breach and Enforcement
Activities and Trends

Samarria Dunson, Esq., CHC, CHPC
HISTORY OF HITECH
NEW SAFE HARBOR
FUSS ABOUT HITRUST
WHAT’S UP WITH NIST?
LIKELY LEGISLATION TO LOOK OUT FOR ON THE HORIZON
What if lawyers and IT professionals spoke the same language?
Cyber Crime Statistics

➢ Data breaches resulted in 36 billion records being exposed in the first three quarters of 2020
➢ The use of malware increased by 358% through 2020
➢ Ransomware usage increased by 435% compared to the previous 2019
➢ July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019
➢ More than 90% of healthcare organizations suffered at least one cybersecurity breach in the previous three years
➢ Since COVID-19, the FBI reported a 300% increase in reported cybercrimes
Cyber Crime Costs

- Cyber crime costs organizations $2.9 million every minute and major businesses lose $25 per minute as a result of data breaches.
- It takes 280 days to find and contain the average cyberattack.
- The average attack costs $3.86 million.
- The U.S. has the world’s highest data breach costs, with the average attack costing $8.6 million.
Cyber Warfare Effectiveness

➢ Well-Funded
➢ Smart
➢ Advanced
➢ Patient

Why U.S. is so susceptible to ransomware:
➢ High profit margin
➢ Vulnerable infrastructure
➢ Default settings
What’s The Deal With Trojans?
Hackers Are Targeting Your Vendors

➢ Third Party Vendors More Vulnerable
➢ Business Associate Agreements
➢ Satisfactory Assurances Down Stream
➢ Termination of Relationship
Top 10 Hacker Conferences of 2020

1. Bsides
2. Hackers on Planet Earth (H.O.P.E.)
3. DEF CON
4. DerbyCon
5. GrrCON
6. SchmooCon
7. THOTOCON
8. NullCon
9. The Hackers Conference
10. 44CON
As Defcon goes virtual, organizers step up efforts to prevent online harassment

The hacker conference’s "Safe Mode" means that many of its attendees will have to concede to being tracked in some form.

Blackhat
Defcon
2020
Now in its 24th year, Black Hat USA is excited to present a unique hybrid event experience, offering the cybersecurity community a choice in how they wish to participate. Black Hat USA 2021 will open with four days of Virtual Trainings (July 31-August 3) conducted in real-time online, with all instructors accessible throughout each class. The two-day main conference (August 4-5) featuring briefings, Arsenal, Business Hall, and more will be a hybrid event—offering both a Virtual (online) Event and a Live, In-Person Event in Las Vegas. See the Conference Highlights below for more details.

CONFERENCE HIGHLIGHTS

TRAININGS

Saturday, July 31 - Thursday, August 5
All 2021 Trainings will be virtual and accessible online from anywhere in the world. Class sizes and labs will be fully interactive and presented live, expanding upon the highly successful virtual model introduced in 2020.

Often found exclusively at Black Hat, these Trainings are taught by experts from around the globe, providing opportunities for newfound technical skill-building for offensive and defensive hackers at all levels.

BRIEFINGS

Wednesday, August 4 & Thursday, August 5
New for 2021, Black Hat briefings will be offered both virtually online and live, In-Person.

Whether you choose to join your colleagues and peers in Las Vegas or online, all briefings general will include access to all recorded briefings during the event and for a full 30 days afterward. No matter how you choose to participate, you won’t miss a single briefing.

FAQ

The Black Hat Team is very excited at the prospect of once again bringing the infoSec community together in person in Las Vegas, while also offering a virtual option for anyone who prefers to participate online.

We’ve created an FAQ to provide basic information about this year’s event, and we will add to this document as more details are confirmed.
Insider Threats
Insider Threats

THE BIGGEST RISK TO YOUR ENTITY IS MOST LIKELY GOING TO COME FROM WITHIN

Types of Threat with Average Cost to Organization

- Employee or contractor negligence ($310,000)
- Criminal and malicious insiders ($760,000)
- Credential theft ($870,000)
Insider Threat:
Behavioral Indicators

➢ Works Odd Hours
➢ Remotely Accesses Entity Systems At Odd Times
➢ Interest in Matters Outside of Their Scope
➢ Unexplained Affluence
➢ Overwhelmed by Life or Career
➢ Unnecessarily Takes Proprietary Information Home
➢ Disregards Policies on Computer Usage/Security
Breaches Affecting 500+ Individuals
Breaches Affecting 500 + Individuals
Via Network Server

<table>
<thead>
<tr>
<th>Year</th>
<th>Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>85</td>
</tr>
<tr>
<td>2017</td>
<td>87</td>
</tr>
<tr>
<td>2018</td>
<td>59</td>
</tr>
<tr>
<td>2019</td>
<td>111</td>
</tr>
<tr>
<td>2020</td>
<td>241</td>
</tr>
</tbody>
</table>
Breach Types 500+

Sept. 2009 – March 2021
- Hacking/IT 37%
- Unauthorized Access/Disclosure 27%
- Theft 25%
- Loss 6%
- Other 2%
- Improper Disposal 3%

Jan. 2021 – March 2021
- Hacking/IT 68%
- Unauthorized Access/Disclosure 27%
- Theft 3%
- Loss 2%
Breach Locations 500+

Sept. 2009 – March 2021
- Emails 21%
- Paper Records 18%
- Network Server 22%
- Laptop 10%
- Other 9%
- Desktop Computer 9%
- EMR 6%
- Portable Electronic Device 4%
- Unknown 1%

Jan. 2021 – March 2021
- Email 37%
- Paper Records 8%
- Network Server 38%
- Laptop 2%
- Other 5%
- EMR 6%
- Portable Electronic Device
- Desktop Computer
- Unknown 1%
BREACHES OF 500+ CURRENTLY UNDER INVESTIGATION IN ALABAMA

4 Separate Entities:

- Unauthorized Access/Disclosure Relating to Email (670)
- Hacking/IT Incident of Network Server (391,472)
- Hacking/IT Incident Relating to Email (501)
# Recent Enforcement Action

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Fine</th>
<th>Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2020</td>
<td>Lifespan</td>
<td>$1,040,000</td>
<td>Failure to encrypt laptops, lack of device and media controls, and failure to comply with business associate agreement requirements</td>
</tr>
<tr>
<td>July 2020</td>
<td>Athens Orthopedic Clinic</td>
<td>$1,500,000</td>
<td>Failure to implement security measures, maintain policies and procedures, train their workforce and enter into Business Associate Agreements</td>
</tr>
<tr>
<td>August 2020</td>
<td>Beth Israel Lahey Health Behavioral Services</td>
<td>$70,000</td>
<td>Failure to timely provide medical records to patient’s personal representative</td>
</tr>
<tr>
<td>September 2020</td>
<td>St. Joseph’s Hospital and Medical Center</td>
<td>$160,000</td>
<td>Failure to comply with right of access provisions</td>
</tr>
<tr>
<td>September 2020</td>
<td>NY Spine Medicine</td>
<td>$100,000</td>
<td>Right of access violations and failure to charge reasonable fees as required</td>
</tr>
<tr>
<td>October 2020</td>
<td>Aetna</td>
<td>$1,000,000</td>
<td>Impermissible disclosures, failure to comply with the minimum necessary rule, and failure to comply with administrative, physical and technical safeguards</td>
</tr>
<tr>
<td>October 2020</td>
<td>City of New Haven, CT</td>
<td>$202,400</td>
<td>Failure to terminate former employee access and failure to conduct enterprise-wide Risk Analysis</td>
</tr>
<tr>
<td>January 2021</td>
<td>Banner Health</td>
<td>$200,000</td>
<td>Right of access violations and failure to charge reasonable fees as required</td>
</tr>
<tr>
<td>January 2021</td>
<td>Excellus</td>
<td>$5,100,000</td>
<td>Failure to conduct enterprise-wide Risk Analysis, failure to implement risk management, information system review and access controls</td>
</tr>
<tr>
<td>March 2021</td>
<td>Arbour</td>
<td>$65,000</td>
<td>Failure to comply with right of access provisions</td>
</tr>
</tbody>
</table>
Recurring HIPAA Compliance Issues

- Individual Right of Access
- Risk Analysis
- Access Controls
- Audit Controls
- Reviewing System Activity
- Business Associate Agreements
- Breach Notification Requirements