# LIHIMA

Long Island Health Information Management Association

September 9, 2020

41st Educational Meeting and Installation Luncheon

# LEGAL UPDATE

Robert F. Elliott, Esq.
Bartlett LLP

# OVERVIEW OF PRESENTATION

- 21st Century Cures Act
- Information Blocking
- CIOX Decision
- Keeping Up with Technology
- Release of Information
- Privacy is More than PHI
- Health Care Proxies and ROI
- Rules Related to Deidentifying and Redacting
- Common Everyday Issues
  - What exactly is the legal EMR
  - What do we turn over
  - Audit Logs, Meta Data
  - EBT of IT People
  - OMH Records
  - Covid 19

# 21ST Century Cures Act

Intended to **“CURE”** limitations in HIPAA and HITECH

# 21ST Century Cures Act

## HISTORY

- Signed into Law on December 13, 2016 by President Obama
- Bipartisan Bill passed by a Republican Congress and signed by a Democratic President

# 21ST Century Cures Act

## GOALS

- Funds the acceleration of research and to prevent and cure serious illnesses (FDA uses Real World Evidence to push approval process along)
- Accelerates drug and medical device development
- Attempts to address the opioid abuse crisis
- Tries to improve mental health service delivery

# 21ST Century Cures Act

## HEALTH INFORMATION MANAGEMENT IMPLICATIONS (HIM)

- The act pushes for greater interoperability
- Adopts electronic health records in the human services setting

# 21ST Century Cures Act

## LOW RISK MEDICAL DEVICES

- The act bars the FDA from regulating mobile health apps designed to maintain or encourage a healthy life style if not related to a diagnosis, prevention or treatment of disease. Essentially bars the FDA from regulating FIT BIT devices and the like.

# 21ST Century Cures Act

## THERE ARE SOME FDA APPROVED DEVICES

- Bio-Gaming – a YuGo Microsoft connect based physical therapy system. Physiotherapists create personalized gamified routine for patients. Can be connected to an X-Box or a computer.
- Dario – a glucometer which sinks to a phone app.
- Triggerfish – helps physicians track progress of glaucoma in patients.
- Quell – A wearable pain relief device that stimulates nerves to treat chronic pain.

# 21ST Century Cures Act

## What are RWD and where do they come from?

- Real-world ***data*** is the data relating to patient health status and/or the delivery of health care routinely collected from a variety of sources. RWD can come from a number of sources, for example:
- Electronic health records (EHRs)
- Claims and billing activities
- Product and disease registries
- Patient-generated data including in home-use settings
- Data gathered from other sources that can inform on health status, such as mobile devices

# 21ST Century Cures Act

## What is RWE?

- Real-world ***evidence*** is the clinical evidence regarding the usage and potential benefits or risks of a medical product derived from analysis of RWD. RWE can be generated by different study designs or analyses, including but not limited to, randomized trials, including large simple trials, pragmatic trials, and observational studies (prospective and/or retrospective).

# 21ST Century Cures Act

## HIPAA Implications

- Provided patient or other qualified person consents, PHI, can be disclosed to researchers
- This authorization may be revoked in writing any time.
- Annual reauthorization is not required but patient is to be sent a copy of his authorization annually nonetheless.
- If revoked, covered entity may still continue to disclose information previously disclosed to maintain integrity of research.
- PHI may be disclosed for research purposes for very limited purposes, if there is prior IRB approval (check with legal counsel - **very sticky**)

# 21ST Century Cures Act

**BEWARE**

**THE FINE PRINT IN THE TERMS OF USE FOR MEDICAL DEVICES!**

# 21ST Century Cures Act

https://www.fitbit.com/global/us/legal/privacy-policy#how-info-is-shared

# Information Blocking

# Information Blocking

- **“WE ARE STILL WORKING ON HOW [INFORMATION BLOCKING RULES] WOULD BE ENFORCED”**

  ONC NATIONAL COORDINATOR DON RUCKER, MD

  JUNE 2020

# Information Blocking

- What is Information Blocking
  - Information blocking is a practice by a health IT developer of certified health IT, a health information network, a health information exchange, or a healthcare provider that, except as required by law or specified by the Secretary of Health and Human Services (HHS) as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of Electronic Health Information (EHI).

# Information Blocking

- Examples
  - Section 4004 of the Cures Act specifies certain practices that could constitute information blocking:
    - Practices that restrict authorized access, exchange or use, including transitions between certified health information technologies – example – upgrading to a new MRI system with resultant inability to migrate all data to new system.
    - Implementing Health IT in a non-standard way that is likely to substantially increase the complexity or burden of accessing, exchanging or using EHI.
    - Implementing Health IT in ways that are likely to restrict access with respect to exploiting complete information sets or in transitioning between health IT systems.
    - Implementing Health IT that might lead to fraud, waste or abuse involving care delivery enabled by health information technology – example – selling mobile medical device data.

# Information Blocking

- There are exceptions
  - Preventing harm
  - Privacy
  - Security
  - Infeasibility
  - Affecting Health IT performance

# Information Blocking

- Exceptions that might implicate your job:
  - It will not be information blocking to limit the content of a response to a request for access, exchange, or use of EHI for the manner in which the request is fulfilled provided certain conditions are met.
  - It will not be information blocking to charge a fee that results in a reasonable profit margin for accessing, exchanging, or using EHI.
  - It will not be information blocking for an actor to license interoperability elements of EHI to be accessed, exchanged or used.

# Information Blocking

- Complaints related to information blocking are submitted to the Office of National Coordinator for Health Information Technology.

# CIOX Decision

# CIOX Decision

- On January 23, 2020, the Federal District Court of the District of Columbia invalidated a provision in the 2013 HIPAA omnibus rule regarding the format for the transmittal of protected health information to third parties as requested by a patient.
- The decision declared unlawful HHS 2016 guidance which extended to third parties, such as insurers and law firms, the limits on charges for copies of PHI that applied to medical record requests made by a patient for use by the patient.

# CIOX Decision

- CIOX is a medical records vendor which contracts with health care suppliers nationwide to maintain, retrieve and produce patient's medical records.
- CIOX challenged the 2016 guidance successfully.
- CIOX also challenged two additional aspects of the 2016 guidance regarding the types of labor costs that are recoverable under the rates charged to patients and how the patient rate is to be calculated.
- The court acknowledged that labor costs which should be included in the rate the patient is charged, included skilled technical staff time spent to create and copy the file, such as compiling, extracting, scanning and burning PHI to media.

# CIOX Decision

- The Office of Civil Rights issued a notice on January 28, 2020 addressing individuals right of access to their health records.
- The fee limitations previously described in the 2016 guidance will only apply to an **individual** request to access to their own records.
- It does not apply to an individuals request to transmit records to a third party. However, more rigorous state laws such as in New York were unaffected by this decision. As a consequence, state law continues to control in States such as New York with more onerous rules.

# CIOX Decision

- New York Law
  - Providers are required to provide access to medical records and copies of records to qualified persons.
  - Qualified persons include the patient or guardian.
  - Qualified persons also include executors and administrators of the estate and if there is no will to the distributees of the estate.(Without letters)
  - An attorney representing the qualified person is also a qualified person provided the attorney has a signed power of attorney.
  - Healthcare providers, insurance companies, other corporate entities and attorneys without a power of attorney are not deemed qualified persons.
  - Providers are permitted to charge reasonable fees to recover costs for copying.
  - Except under very narrow  circumstances, where a qualified person may not be able to afford the costs, reasonable charges for paper copies shall not exceed .75 cents per page.

# CIOX Decision

- A local Medical Center through its 3rd party vendor charges the following: a $6.50 flat fee for a patient no matter what method of delivery
- Attorney representing the patient .75 cents per page up to $950.00 cap.
- Defense attorney $1.50 per page – no cap
- Insurance company $1.50 per page – no cap
- Access for patient care is free

# CIOX Decision

- HHS Office of Civil Rights May, 2019 Fact Sheet
  - OCR has authority to take enforcement action in a myriad of ways including:
    - Failure to disclose a copy of electronic PHI to either a covered entity, the individual or the individual's designee to satisfy a covered entities obligations regarding the form and format and the time and manner of access.
    - Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

# Keeping Up With Technology

- Develop a policy related to medical and nursing staff use of texts. Images from diagnostic tests are being sent by text.
- Develop a policy related to staff use of social media.
- Develop a policy about remote access to protected health information.
- Develop a policy related to TeleHealth disclosures, privacy and security.

# COVID AND PRIVACY

- U.S. Department of Health and Human Services Office of Civil Rights has relaxed HIPAA requirements and HITECH regulations in response to the Covid 19 pandemic.
- Health care providers may use popular applications to deliver TeleHealth, as long they are not “non-public facing”.

# COVID AND PRIVACY

- Examples of non-public facing video chat applications include:
  - Apple Facetime
  - Facebook Messenger Video Chat
  - Google Hangouts Video
  - Zoom
  - Skype

# COVID AND PRIVACY

- Example of public facing text based applications include:
  - Signal
  - Gabber
  - Facebook Messenger
  - Google Hangouts
  - Google Whats App
  - I-Message

  These would be prohibited under the relaxed rules.

# COVID AND PRIVACY

- Covered healthcare providers may seek additional privacy protections by using vendors that are HIPAA compliant.
- Examples of HIPAA compliant vendors:
  - Skype for Business/Microsoft Teams
  - Zoom for Health Care
  - Go To Meeting

# COVID AND PRIVACY

- Medicare patients may be cared for via TeleHealth technology. Are your parents tech savvy ?
- Healthcare providers may offer TeleHealth services to patients located in their homes and outside of designated rural areas.
- Medicare and Medicaid services will reimburse TeleHealth visits in lieu of many in-person appointments.
- Relationship between patient and Provider.
  - During the COVID 19 emergency, physicians may see both new and established patients for telehealth and other visits furnished using communications technology

# COVID AND PRIVACY

Prescribing Controlled Substances

- The DEA has allowed for the prescribing of controlled substances during the emergency:
  - A practitioner can prescribe a controlled substance to a patient using telemedicine, even if the patient is not at a hospital or clinic registered with the DEA.
  - Qualifying practitioners can prescribe Buprenorphine to new and existing patients with opioid use disorder based on a telephone evaluation.

# HOW PRIVATE IS PRIVATE?

DEIDENTIFICATION

- “Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.”
- “If inferences may be drawn from any personal information to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predisposition, behavior, attitudes, intelligence, abilities and aptitudes” may not be deidentified enough.

# HOW PRIVATE IS PRIVATE?

| | HIPAA | HIPAA: Privacy and Security | HITECH | GDPR | CCPA |
|---|---|---|---|---|---|
| **Date** | •Compliance required by all parties within **24 months of 8/21/1996 signing** | •**4/14/2003 privacy rule** compliance required •**4/20/2005 security rule** compliance required | •**2/17/2009 signed and 2/18/2009 effective** | **4/14/2016** adopted, **5/25/2018 enforceable** | Passed in June, 2019 and **effective 1/1/2020** |
| **Jurisdiction** | •Health plans, providers and healthcare clearinghouses | •Covered entities (providers, payors, clearinghouses) & biz associates who confront protected health info while providing or paying for | •Covered entities and their biz associates •Requires biz associates to comply with HIPAA security rule and privacy rule | •All companies with >250 employees that deal with EU citizen data, in person or online | •Any company doing any business in CA that meets at least one of three condit: • >$25m revenue •>50k consumers' data •>50% of revenue from |
| **Gist** | •Est data mgmt and admin protocols to standardize electronic health transactions •Employer Id Number (EIN) & National Provider Identifier (NPI) | •Privacy Rule defines protected health info and who gets access/why •Security Rule puts admin, physical and tech safeguards up to ensure the integrity of protected health info | •Establishes 4 categories of violations and penalties •Ends auto-exoneration for ignorance •No penalties if violations corrected within 30 days | •Scope and purpose of data collection to be presented for affirmative consent •Broad definition of personal •Consumers can have both privacy and access | •Consumers have the right to know what data has been collected, by whom and to what end. •Right to opt out, to delete, and to protection from discrimination |
| **Zeitgeist** | •Dawn of the EHR •Save costs, thwart fraud and improve quality in Medicare/Medicaid by establishing/encouraging the use of streamlined electronic protocols | •Populace is concerned about the potential for discrimination on basis of health •Providers concerned about obstruction | •"Meaningful use" to spur EHR •With great stimulus comes great responsibility... •Puts onus of compliance on covered entities/biz associates where formerly ignorance=exoneration | •Lack of gov't oversight and porous privacy protections across the internet allowed companies and sovereigns to amass troves of personal data and deploy it to steer behavior | •Cambridge Analytica introduces data as a weapon, reveals susceptibility to psychosocial manipulation •Bad actors capitalizing on the speicifc vulnerabilities an individual's digital/physical life |
| **Intent** | •#1 aim was to make insurance portable bet jobs, ensure continuity in group/individual markets •Ensure security via standardization, easy to monitor protocols | •Seeks to establish and protect individual's privacy rights w/ re to protected health information, without inhibiting the free flow of info necessary in provision of/payment for healthcare | •Sought to hasten adoption of EHRs •Gave HIPAA teeth: expands definition of violation, increases # and extent of allowable fines, makes HIPAA security risk assessmet a condition of meaningful use | •"Digital single market," premised on fair competition, sweeping consumer protections •Contracts may govern specific engagements •But data rights default to individual at contract expiry | •Protection from the unseen and unwelcome influence of targeted propaganda •Consumers can't resist what they do not know exists, disclosure of data collection means & ends identifies the exogenous force |

Source: Piper Jaffray Research

# HOW PRIVATE IS PRIVATE?

California Consumer Privacy Act (CCPA)

Effective January 1, 2020.

- Businesses must disclose what information they collect, what business purpose they serve and any third parties with whom they share that data.
- Businesses will be required to comply with official consumer requests to delete that data.
- Consumers can opt out of their data being sold, and businesses cannot retaliate by changing the price or level of service.
- Businesses can, however offer financial incentives, (for being allowed to collect data).
- California authorities are empowered to fine companies for violations.
- Is this coming to New York?

# HOW PRIVATE IS PRIVATE?

Like California Emissions Standards, because so many people live in California and there are so many consumers, we can expect most Big businesses such as CVS to begin to comply. The consumer opt out takes place at the point of sale.

# HOW PRIVATE IS PRIVATE?

- Personal information according the CCPA is “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly, with a particular consumer or household.”
- The act recognizes a “broad list of characteristics and behaviors, personal and commercial, as well as inference drawn from this information” that can be used to identify an individual.

Examples:

- Name, address, phone number, e-mail address, social security number, drivers license number, etc.
- Biometric information, such as DNA or fingerprints.
- Internet activity, including but not limited to browsing and search history.
- Geo location data.
- Professional or employment related information
- Education information
- Inferences drawn from any of the above examples that can create a profile about a consumer reflecting the consumer’s preferences.

# HOW PRIVATE IS PRIVATE?

Fines and Penalties

- $2,500.00 fine for unintentional and $7,500.00 for intentional violations of the act.
- $100.00 to $750.00 per incident, per consumer – or actual damages, if higher, for damage caused by a data breach.
- A business is only in violation of the CCPA if it fails to cure any alleged violation of the CCPA within thirty days after being notified of alleged noncompliance.
- A limited narrow private right of action for certain data breaches is allowed, unlike with HIPAA.

# HOW PRIVATE IS PRIVATE?

General Data Protection Regulation (GDPR)

A regulation in the EU on data protection and Privacy. It was enacted on May 25, 2018.

Primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business.

It describes  personal data as information that relates to an identified or identifiable individual.

Unless an individual provides informed consent to permit data processing their personal identifiable information, it may not be processed unless:

- Consent has been given.
- To fulfill contractual obligations.
- To comply with a data controller's legal obligations.
- To protect the vital interests of a data subject or other individual.
- To perform a task in the public interest or an official authority.

# HOW PRIVATE IS PRIVATE?

Google Data Mining Scandal

- Google secretly monitors millions of school kids, lawsuit alleges.
- A lawsuit filed by New Mexico's Attorney General alleges that Google uses its dominance in schools to "spy on millions of future customers" tracking the digital lives of kids as early as kindergarten.
- Google using its purely education tool – Google Education – now used by more than 80 million educators and students, gives the company access to their digital lives and personal data. More than 25 million students and teachers also use Chrome Books, laptops that run on Google's operating system.
- New Mexico alleges that the company's data mining of kids violates the children's online privacy protection act, which requires companies to get a parent's consent before collecting the name, contact information and other personal details from a child under 13.

# DEIDENTIFICATION AND REIDENTIFICATION

- The HIPAA privacy rule protects most “individually identifiably health information” held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper or oral.
- The privacy rule calls this information Protected Health Information (PHI).

# DEIDENTIFICATION AND REIDENTIFICATION

Protected Health Information

- The individuals past, present or future physical or mental health or condition.
- The provision of healthcare for the individual
- The past, present or future payment for the provision of healthcare to the individual and that identifies the individual for which there is a reasonable basis to believe can be used to identify the individual.
- Examples include: name, address, birth date, etc.

# DEIDENTIFICATION AND REIDENTIFICATION

Deidentification and its rationale

- The rapid adoption of health information technologies in the United States has accelerated their potential to facilitate beneficial studies that combine large, complex data sets for multiple sources.

The process of deidentification, by which identifiers are removed from the health information, mitigates privacy risks to individuals and supports the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research and other endeavors.

The Privacy rule permitting deidentificaiton allows a covered entity to create information that is not individually identifiable by following the deidentification standard and implementation specifications in Section 164.514(a)-(b).

# DEIDENTIFICATION AND REIDENTIFICATION

There are two permissible ways to deidentify protected health information.

Expert determination standard

HIPAA Section 164.514(b)(1)

Applies statistical or scientific principles for rendering information not individually identifiable.

Applying those principles and methods to determine that the risk is very small that the information can be used, alone, or in combination with other reasonably available information by an anticipated recipient to identify a person.

Document the methods and results of the analysis that justifies such determination.

# DEIDENTIFICATION AND REIDENTIFICATION

## The second way is the “Safe Harbor” method

Eighteen discrete identifiers of the individual or of the relatives, employers, or household members of the individual are removed:

Name

All geographic subdivision smaller than a state

All elements of dates that are directly related to the individual, including birth date, admission date, and so on.

Telephone numbers

Vehicle identifiers and serial numbers, including license plates

Fax numbers

Device identifiers and serial numbers

Email addresses

URLs

Social Security Number

IP addresses

Medical record number

Biometric identifiers, including finger and voice prints and DNA information

Health plan numbers

Photogrpahs

Account number

Any other unique identifying number, characteristic or code

Certificate or license numbers

# DEIDENTIFICATION AND REIDENTIFICATION

Satisfying either method would demonstrate that a covered entity has met the standard in Section 164.514(a) above.

Deidentified information is no longer PHI.

Deidentification may lead to information loss which may limit the usefulness of the resultant health information in certain circumstances.

This deidentified information is sold and exchanged and otherwise use for a myriad of commercial and scientific purposes.

# DEIDENTIFICATION AND REIDENTIFICATION

Reidentification

Assign a unique code to the set of deidentified health information to permit reidentification by the covered entity.

# DEIDENTIFICATION AND REIDENTIFICATION

Risk of reidentification for an evil purpose:

Data mining companies can match data sets which are inadvertently exposed resulting in a massive data breach to reidentify patients within the data mining companies data base.

Also, patients with unique and rare diseases whereby the inclusion of a rare disease diagnosis is in the data set maybe become a unique identifier all by it self.

Including genomic data in the data set increases the complexity of making the data set deidentified because genomic data is a patient identifier – everyone's DNA is unique!

Source: PiperJaffray company note November 14, 2019

# COMMON EVERYDAY PROBLEMS

What exactly is the legal EMR?

- Managing requests for audit logs and meta data
- EBT of IT or HIM  people
- Statutes permit certification of the records to substitute in the place of a witness to authenticate the data
- Responding to State agencies for medical record requests: IE, OMH, DOH, OPMC, OPD, OIG, OCR – you better get it right the first time
- Making sure records are full and complete for litigation purposes, especially mental health records and records related to drug and alcohol treatment

# Surrogates and ROI

New York's Family Health Care Decisions Act (PHL Chapters 29-cc and 29-ccc) was enacted in 2010

- It allows a patient's family member or close friend to make healthcare decisions for a patient who is in a **hospital** or **nursing home**, if the patient lacks decision making capacity who did not leave prior instructions or sign a health care proxy.
- This "surrogate" decision maker would also be empowered to direct the withdrawal or withholding of life sustaining treatment, including consenting to a DNR order if standards listed in the statute are satisfied.

# Surrogates and ROI

- Who are Surrogates:
  - Legal guardian appointed under Article 81 of the Mental Hygiene Law.
  - Spouse or domestic partner
  - Adult child
  - Parent
  - Brother or sister
  - Close friend if age 18 or over, or a relative other than listed above who can attest to regular contact with the patient so as to be familiar with the patient's activities, health, religious and moral beliefs.
- The surrogate may make all healthcare decisions in a hospital or nursing home that the adult patient could have made, including but not limited to signing a consent to release information.

# QUESTIONS?