Post & Schell P.C.
ATTORNEYS AT LAW

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

# Are You Ready For The 21st Century Cures Act?

Cynthia A. Haines
Principal and Co-Chair
Information Privacy & Security Practice Group,
Post & Schell, P.C.

September 28, 2022

# The 21st Century Cures Act

- Passed by Congress in 2016.
- Calls for electronically accessible health information to be accessed, exchanged, and used without special effort on the part of the user.
- The Office of the National Coordinator of Health Information Technology (ONC) states that the rule puts patients in charge of their health records, which is a key piece of patient control in healthcare.

# Interoperability

- **May 1, 2020**: The ONC and Centers for Medicare and Medicaid Services (CMS) published final rules to implement interoperability requirements.

- **Interoperability**: The ability for health care providers, payors, and health information exchanges to share and access health information data across systems to facilitate health care delivery and management.

# Interoperability

- Additionally, patient control is at the center of the Health and Human Services (HHS) work toward a value-based healthcare system.

- The final rule promotes innovation in the healthcare technology ecosystem to deliver better information, more conveniently, to patients, clinicians, and payers.

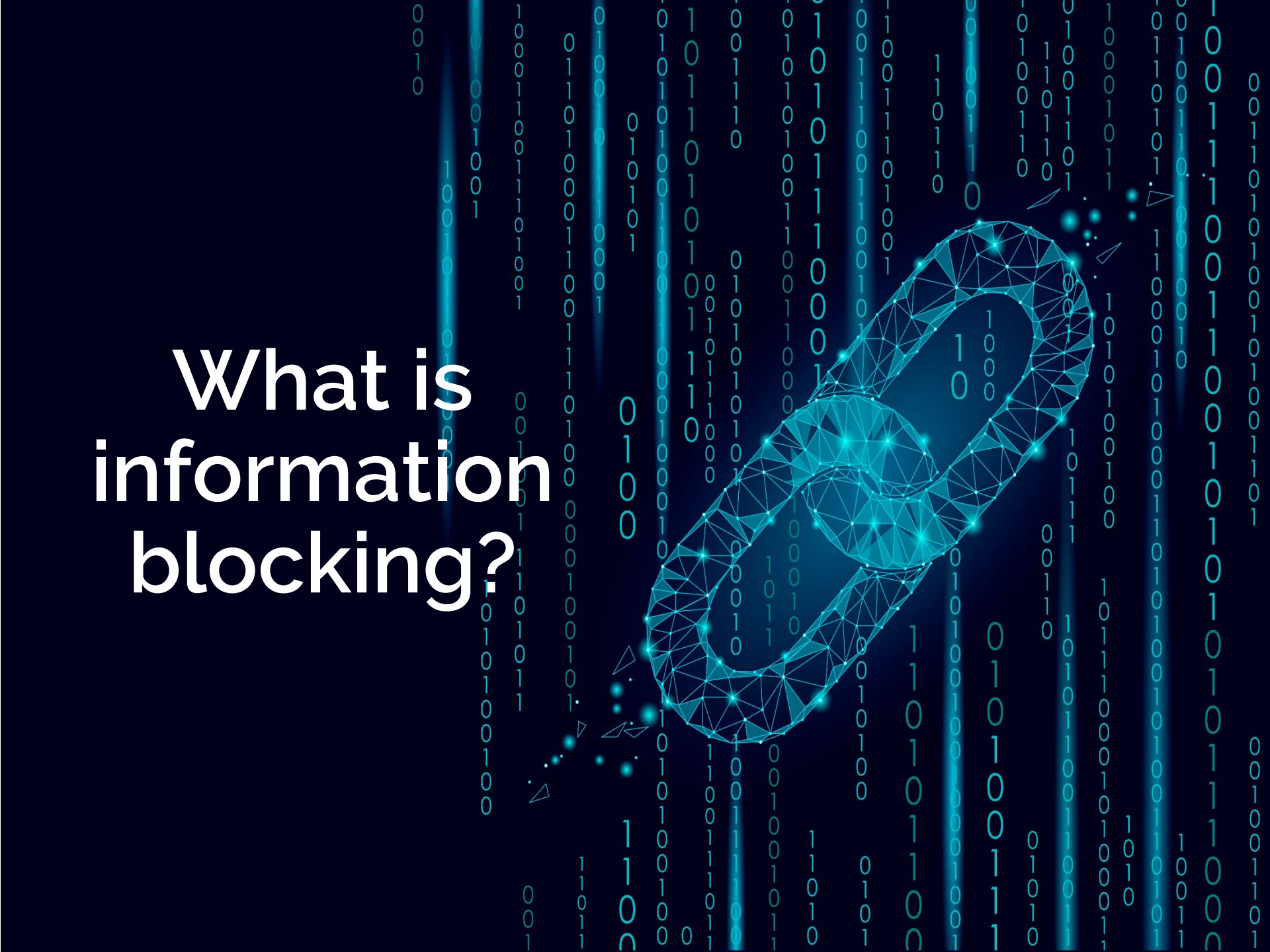
# What is Electronic Health Information?

- ONC defines electronic health information **(EHI)** as the electronic protected health information **(ePHI)** included in a designated record set (as defined in the Health Insurance Portability and Accountability Act) regardless of whether the records are used or maintained by or for a covered entity.

- This includes records received from other entities.

- EHI does NOT include psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

# What is information blocking?



# Information Blocking

- **Information Blocking**: A practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI).
  - Includes a health care provider that knows such practice is unreasonable and is likely to do any of the above.
  - Includes a provision requiring that patients can access all of their electronic health information, structured and/or unstructured, at no cost.
  - A practice is not information blocking if it is required by law or if it satisfies an exception.

# Information Blocking

**The American Medical Association** (AMA) describes information blocking this way:

*"Information blocking can occur in many forms. Providers can experience information blocking when trying to access patient records from other providers, connecting their EHR systems to local health information exchanges (HIEs), migrating from one EHR to another, and linking their EHRs with a clinical data registry. Patients also can experience information blocking when trying to access their medical records or when sending their records to another provider."*

# Who Can Information Block?

- The Cures Act defines three categories of "actors" who can block information:
  - Healthcare providers.
  - Developers of certified health information technology.
  - Health information networks or health information exchanges.

# Who Can Information Block

- Providers include but are not limited to:
  - Skilled nursing facilities.
  - Home health entities or other long-term care facilities, practitioners, or clinicians.
  - Includes acute and long-term acute care hospitals, inpatient rehabilitation facilities.

# Information Blocking

- Formally restricting access, exchange, or use of EHI, such as through contractual terms, health information sharing policies, or organization policies or procedures:
  - *Example*: A facility's internal policies or procedures that require staff to obtain an individual's written consent before sharing the resident's EHI with unaffiliated providers for treatment purposes even though obtaining such consent is not required by state or federal law.
- Unnecessarily slowing or delaying access, exchange, or use of EHI, or otherwise limiting the timeliness of health information access or exchange.
- Charging an individual, their personal representative, or another person or entity designated by the individual for electronic access to the individual's EHI.

# Compliance

- Just because an action prevents, materially discourages, or interferes with the access, exchange, or use of EHI does not mean the actor is guilty of information blocking. A review of the facts and circumstances need to be considered. Additionally, the rule provides some exceptions.
- Although LTC providers are obligated to identify blocking occurrences, their primary responsibility under this rule will be to ensure patients or their representatives have timely access to their electronic medical records.
- Timely is defined in the rule as within ten (10) business days or provide the requestor with an explanation for the delay. However, in accordance with federal regulations, skilled nursing facilities (SNFs) are required to respond within 24 hours to two days.

# Examples

- High-risk information blocking actions include interfering with:
  - Residents who seek to access their own EHI.
  - Providers who seek EHI for treatment or quality improvement.
  - Payers who seek EHI to confirm a clinical value.
  - Resident safety and public health.

# Example

- A Facility, for instance, may have a policy that restricts access to resident records in the EHR for a certain amount of time or until all documents are signed.
- Even if residents or their representatives are not aware there is a delay between when the timely completion of documents by providers are available to the facility and when they are made available to the patient, a facility that is merely "likely" to interfere with the access, use or exchange of EHI could be considered information blocking.

# Examples

- Practices that impose formal restrictions on authorized access, exchange or use of EHI under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law:
  - *Example*: Your entity's policy requires staff to obtain a resident's written consent before sharing any EHI with unaffiliated providers for treatment purposes
  - *Example*: Not allowing the resident's representative to look at (access) the EHR documentation of a resident's fall from the night before until the Director of Nursing (DON) is available

**To Do**: Review facility policies and procedures for practices that impose formal restrictions.

# Examples

- Practices that impose informal restrictions on authorized access, exchange or use of EHI under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law:
  - *Example*: Not responding to a resident representative's request for copies of the resident's records for three weeks and providing no explanation for the delay. However, if the delay is because the clinician hasn't reviewed the documentation yet, this, too, will be considered information blocking.

# Examples

- *Example*: Failure to provide copies of or send a copy of certain reports to a clinical consultant who will be seeing the resident in time for the resident's consultation visit.
- *Example*: A healthcare provider has the capability to provide same-day access to EHI in a form and format requested by a resident or a resident's healthcare provider but takes several days to respond.

**To Do**: Explore daily workflow processes related to exchanging information for any informal restrictions or unstated policies that are currently in use. Determine if these could be perceived as information blocking and take action where applicable.

# Examples

- Implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging or using EHI:
  - *Example*: Selecting an EHR that is unable to exchange data electronically. Vendors may need to be reminded that they are subject to the rules.
  - *Example*: Blocking certain data elements within the EHR from being interoperable, i.e., electronically transferred, (except under local/state law), e.g., Incident documentation, behavior tracking reports.

**To Do**: Evaluate EHR's limitations and settings that could be perceived as information blocking and take action where applicable on the findings.

# Examples

- Implementing health IT capabilities in ways that are likely to restrict the access, exchange or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems.
- This would include acts that make transitions between health information technologies more challenging (e.g., an EHR vendor charging excessive fees or using tactics to delay a practice's switch from their EHR to another vendor's EHR):
  - *Example*: EHR vendor announces that support for the EHR will end as of Dec. 31, and the healthcare organization must transfer the resident records by that date or pay a legacy system activation fee equivalent to two times the current annual license fee.
  - *Example*: Prior EHR vendor exports historical information in a non-usable format (e.g., assessments for every resident are now contained in one excel spreadsheet).

**To Do**: Evaluate termination clauses in current EHR vendor's contract.

# Examples

- Imposing terms or conditions that discourage the exchange of information:
  - *Example*: Unwillingness to send information electronically to a SNF owned by a competing organization.
  - *Example*: Unwillingness to send information electronically to another provider because it would share a process (or form) that the organization considers proprietary.

**To Do**: Evaluate the organization's policies, procedures or practices that could be perceived as information blocking and take action where applicable on the findings.

# Examples

- Acts that lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange and use, including care delivery enabled by health IT:
  - *Example*: Copy/paste from previous notes to avoid the effort of creating a new note.
  - *Example*: EHR vendor releases an updated version of software that includes features that promote electronic sharing of additional data. However, the organization chooses not to implement it.

**To Do**: Evaluate EHR's settings and organizational decisions that could be perceived as information blocking and take action where applicable on the findings. Document all decision making.

# Examples

- Restrictions on access, exchange and use, that may be expressed in contracts, license terms, EHI sharing policies, organizational policies or procedures or other documents that set forth requirements related to EHI or health IT, for example Business Associate Agreements (BAAs):
  - *Example*: Releasing information by paper to payers, while releasing information electronically to treatment providers
  - *Example*: Restricting needed information to a certain group based on competition, e.g., restricting information from being sent to a specialty pharmacy to keep prescriptions in house or with a contracted pharmacy

**To Do**: Review contracts, policies and other documents for language that implies restrictions. Determine if the language could be perceived as information blocking and take action where applicable on the findings.

# Examples

- "Rent seeking" which usually applies to vendors and is the practice of gaining larger profits by manipulating economic conditions or other opportunistic pricing practices:
  - *Example*: Excessively (not FMV with a reasonable profit margin) charging for an update that included pandemic-related data elements to take advantage of the crisis and the need to capture pandemic-related information.
  - **Comment**: OIG/ONC has yet to define what a "reasonable" profit margin is.

**To Do**: Facilities should be aware of this category of information blocking and, if needed, remind the organization's EHR software vendors of this concern.

# Examples

- Discriminatory practices that frustrate or discourage efforts to enable interoperability:
  - *Example*: Exchanging information with an affiliated facility or one in the same network and refusing to send information to a competing non-network facility.
  - *Example*: Exchanging information with physicians that refer residents to the facility but refusing to share information with a physician who rarely refers to the facility and who now has a patient in the SNF.

**To Do**: Evaluate organization's policies, procedures or practices that could be perceived as information blocking and take action where applicable on the findings.

# Information Blocking: Exceptions Overview

- The ONC Final Rule outlines eight exceptions to the definition of information blocking.
- The exceptions are intended to promote two overarching policy goals:
  - Promoting public confidence in the health IT infrastructure by protecting privacy and security of EHI.
  - Promoting competition and innovation in health IT.

# Information Blocking: Exceptions

- **Preventing Harm Exception**: An actor may engage in practices that are reasonable and necessary to prevent harm to a resident or another person.
- This aligns with the HIPAA exception to access related to preventing harm.
  - *Example*: Resident has signs of physical abuse upon return from a weekend pass with the family. Photos of the bruises and interviews with the resident where he stated "they weren't very nice to me" have been documented in the record. The family has asked for copies of the record. The copies provided are redacted for this information.

# Information Blocking: Exceptions

- **Privacy Exception**: An actor can leave a request to access, exchange, or use EHI unfulfilled in order to protect an individual's privacy.
- Aligns with HIPAA's minimum necessary policy and the parameters around personal representatives.
  - *Example*: The resident is competent and has specifically requested that no information be shared with his daughter. His daughter is not paying for any of his care. The daughter requests to see the resident's record. Consistent with current privacy laws, the request is denied.

# Information Blocking: Exceptions

- **Security Exception**: An actor may interfere with the access, exchange, or use of EHI to protect the security of the EHI.
- Aligns with required HIPAA Security measures.
  - *Example*: An organization can only support certain security parameters for exchange, although the exchange requires a higher level of security.
  - *Example*: SNF receives a request to deliver documentation for a recently discharged resident to a local senior community center to provide adult daycare services for the patient. The senior community center asks for these documents to be sent to their generic Gmail account. The SNF offers to place the information on a secured portal for the requestor from the senior community center to access and download, citing concern about the need to secure the information from inappropriate access.

# Information Blocking: Exceptions

- **Infeasibility Exception**: An actor may leave a request to access, exchange, or use EHI unfulfilled due to the infeasibility of the request:
  - *Example*: During a severe hurricane, the healthcare facility loses all power and is unable to electronically transmit information until the power is restored.
  - *Example*: An organization receives a request from a family to create an API to send all data for their mother to them.
    - API is a type of technology that is the foundation of smartphone applications ("apps"), and which has enabled seamless, user-friendly data exchange via apps in the online banking and travel-booking industries.
    - The organization does not have the IT staff to create this API, nor does the SNF have the legal rights to create this for the EHR they are using. For these reasons, they refuse this request, citing this exception.

# How Do APIs in Healthcare Work?

# How Do APIs in Healthcare Work?

1. A patient downloads the health app of her choice.
2. The patient logs into the app and creates a username and password for the app.
3. The patient uses the app to link securely to an API for the health care provider.
4. The app sends a request to the provider asking for access to the patient's medical records.
5. The health care provider's server validates the request coming from its API, fulfills the criteria, and sends back the patient's data in a structured format.
6. The patient can now access health information from the app.
7. The patient repeats steps 3-6 with other health care providers that have granted access to the app.
8. Depending on the app, the patient can now merge the health information from multiple sources, to access all their health information in once place.

# Information Blocking: Exceptions

- **Health IT Performance Exception**: An actor may take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT:
  - *Example*: The facility installed an update which resulted in the inability to log-in to the EHR. A resident's wife asked to see her husband's record during this period. The DON advised that the access would need to occur another day and explained the EHR was down at this time.

# Information Blocking: Exceptions

- **Content and Manner Exception**: An actor may limit the content of its response to, or the manner in which it fulfills, a request to access, exchange, or use EHI:
  - *Example*: An organization contacts a SNF and asks for data via Fast Healthcare Interoperability Resources (FHIR) standards. The SNF responds that it cannot exchange via FHIR standards and proposes instead to share using Clinical Document Architecture (CDA) standards. Both parties agree to this option.

# Information Blocking: Exceptions

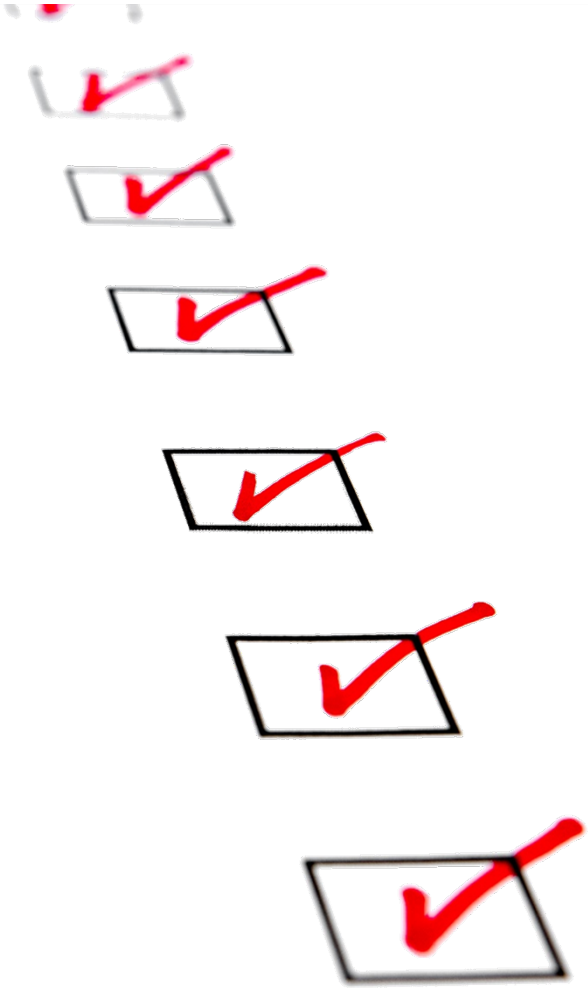
- **Fees Exception**: An actor may charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI.
  - *Example*: The news of a community's success in reducing labor costs becomes known in the community.
    - The IT consultant for another community has asked if they could create the same interfaces since the second community uses the same EHR. The first community can charge a fee for use.
    - Many EHR's prohibit this contractually by requiring the provider to agree that innovation will be shared intellectual property.

# Information Blocking: Exceptions

- **Licensing Exception:** An actor may license interoperability elements for EHI to be accessed, exchanged, or used.
  - *Example*: Community with a number of facilities uses an EHR that is common in the industry.
    - In order to facilitate centralization of certain services within this region, the community has developed interfaces between the facilities and the central office.
    - The central office is able to process all payer requests for copies of records and upload those copies to the payers' portals.
    - At the end of each month, each facility is levied a small charge for the number of requests the central office handled to offset the central office's labor and technology investment costs.

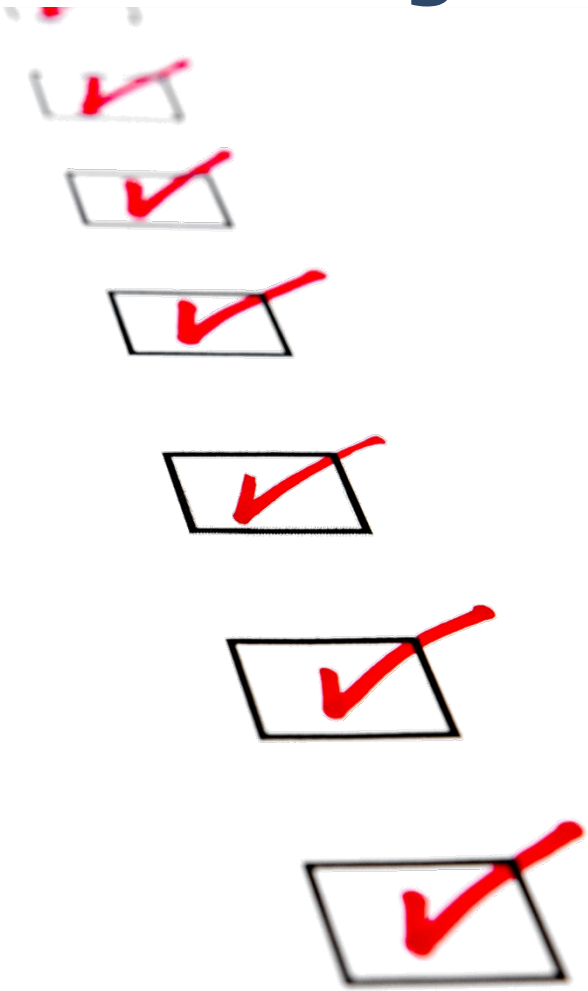
# Best Practices - Information Blocking

- Identify a person to lead this project.
- Review state privacy laws to learn if releasing certain information is allowable.
- Review all policies and procedures for any language that could be perceived to "prevent or materially discourage the access, exchange, or use of EHI.
- Identify all current processes and scenarios for requests for information - from patients, family, attorney, third party app, etc.



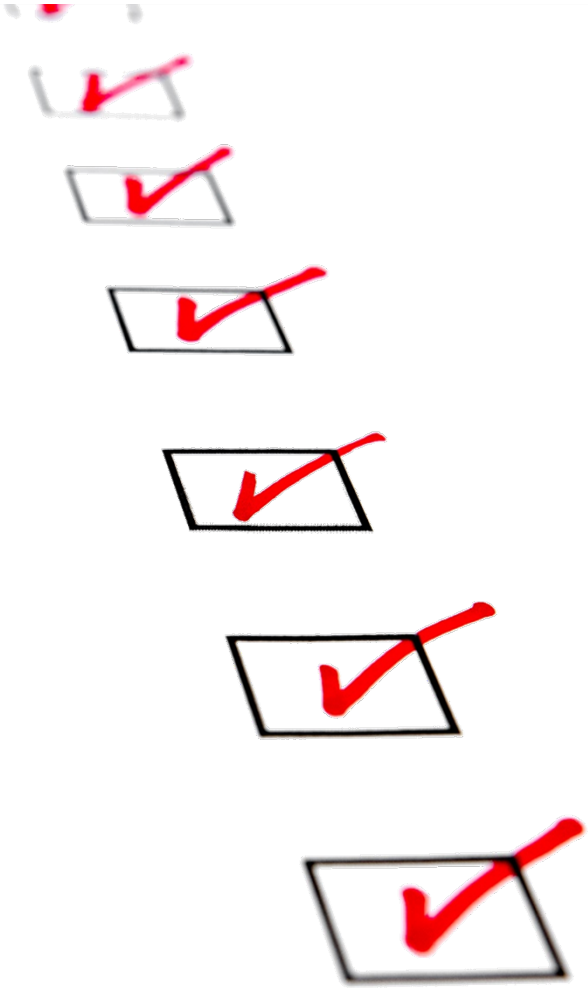
# Best Practices - Information Blocking

- **Designate** a point person(s) for release of information requests.
- **Understand** the composition of your medical record and capabilities for release of information.
- **Create** "how to address" procedures to facilitate release of information for any type of request.
- **Evaluate** and update your compliance infrastructure to provide the information electronically (and securely) and to document/track that this was completed.



# Best Practices - Information Blocking

- Begin providing education to all employees
- Consider creating a patient portal and providing the information through this portal (with ability for patient/resident representative to download any information from the portal)
- Set specific expectations and prepare policies and procedures for access (See, Sample)
- Address any fees: No fees can be charged for access to digital information by residents and/or resident representatives. State regulations may permit charges to be made for copies or placement of EHI on alternative media, such as a jump drive or DVD



# Questions?

# Thank You!

**Cynthia A. Haines**
**Principal & Co-Chair**
**Information Privacy & Security**
**Practice Group**
**Post & Schell, P.C.**

717-612-6051 (Phone)
717-317-3633 (Cell)
CHaines@PostSchell.com
www.postschell.com