COPPERSMITH BROCKELMAN LAWYERS

CHS Community Health Systems

# Navigating Privacy Challenges in Collaborative Care Access

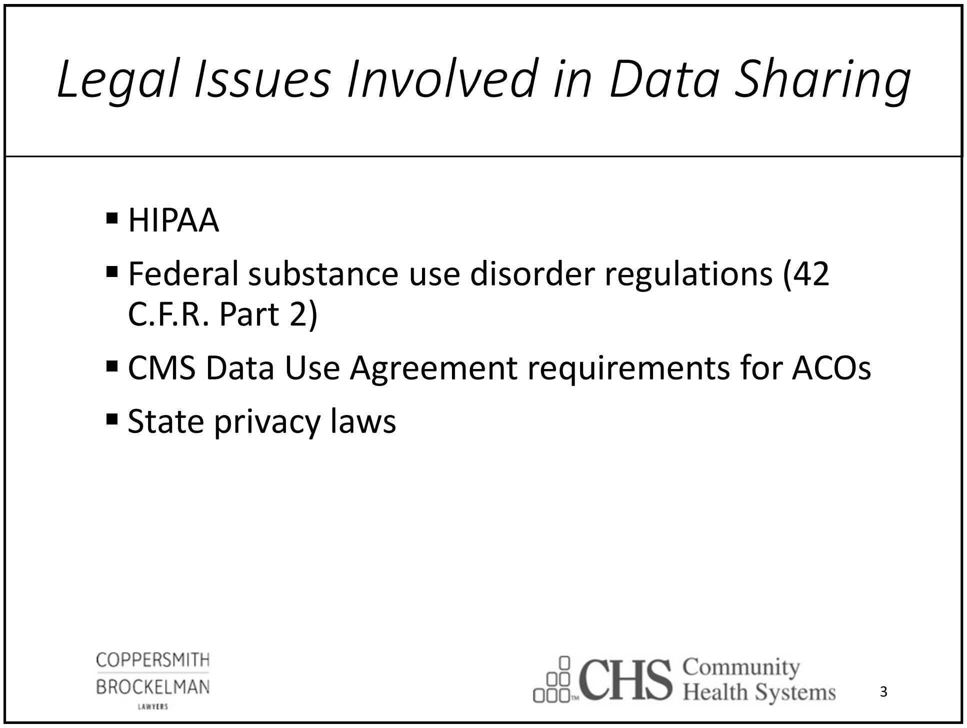
Kristen B. Rosati
Coppersmith Brockelman PLC
krosati@cblawyers.com
602-381-5464

Tyler Golden
CHSPSC, LLC
tyler_golden@chs.net
615-786-8142

Heathyr A. Fields
CHSPSC, LLC
heathyr_fields@chs.net
615-465-7292

## *Disclaimers*

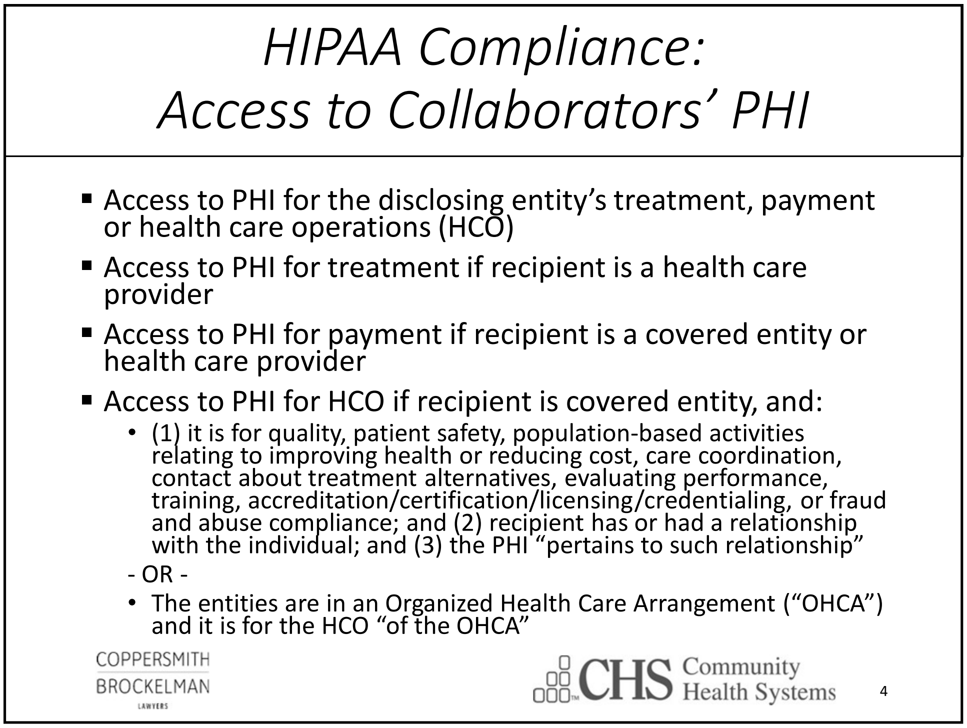
- *Remember this is not legal advice and that this presentation reflects our thoughts and opinions, not those of our employers.*
- *Ask questions as we go.*
- *Have fun.*



# *Legal Issues Involved in Data Sharing*

- HIPAA
- Federal substance use disorder regulations (42 C.F.R. Part 2)
- CMS Data Use Agreement requirements for ACOs
- State privacy laws

3

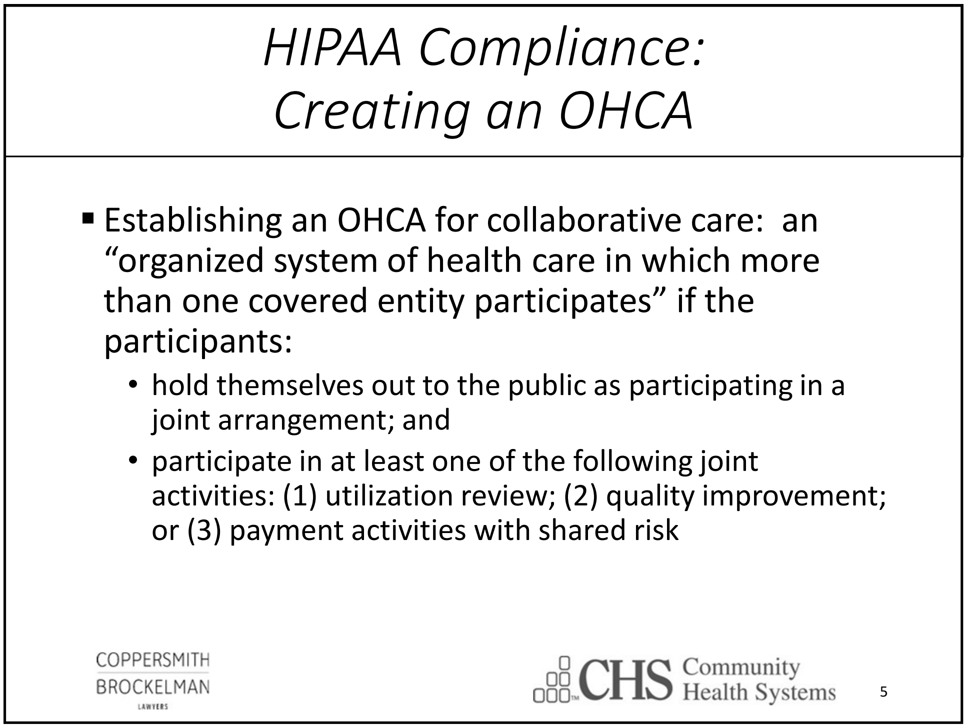


# *HIPAA Compliance: Access to Collaborators' PHI*

- Access to PHI for the disclosing entity's treatment, payment or health care operations (HCO)
- Access to PHI for treatment if recipient is a health care provider
- Access to PHI for payment if recipient is a covered entity or health care provider
- Access to PHI for HCO if recipient is covered entity, and:
  - (1) it is for quality, patient safety, population-based activities relating to improving health or reducing cost, care coordination, contact about treatment alternatives, evaluating performance, training, accreditation/certification/licensing/credentialing, or fraud and abuse compliance; and (2) recipient has or had a relationship with the individual; and (3) the PHI "pertains to such relationship"

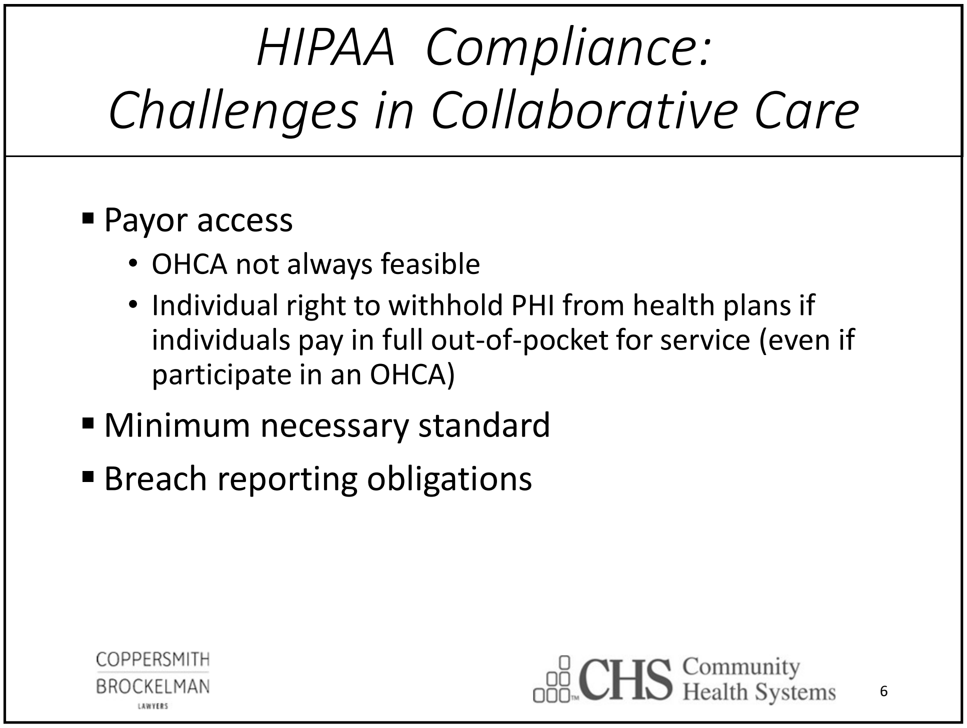
  - OR -
  - The entities are in an Organized Health Care Arrangement ("OHCA") and it is for the HCO "of the OHCA"

4



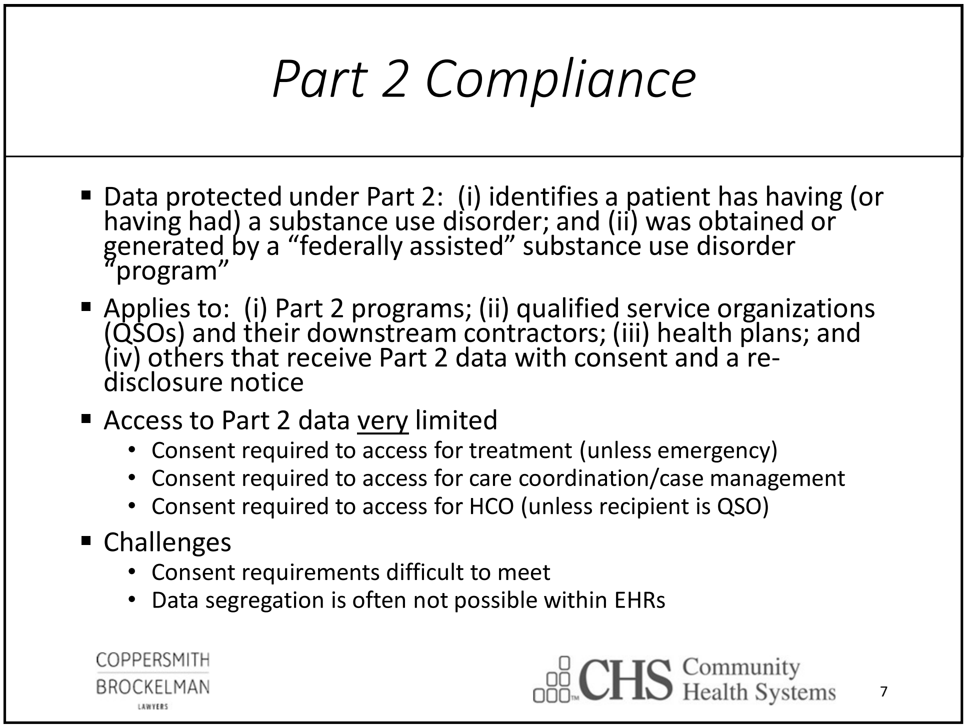
# HIPAA Compliance: Creating an OHCA

- Establishing an OHCA for collaborative care: an "organized system of health care in which more than one covered entity participates" if the participants:
  - hold themselves out to the public as participating in a joint arrangement; and
  - participate in at least one of the following joint activities: (1) utilization review; (2) quality improvement; or (3) payment activities with shared risk



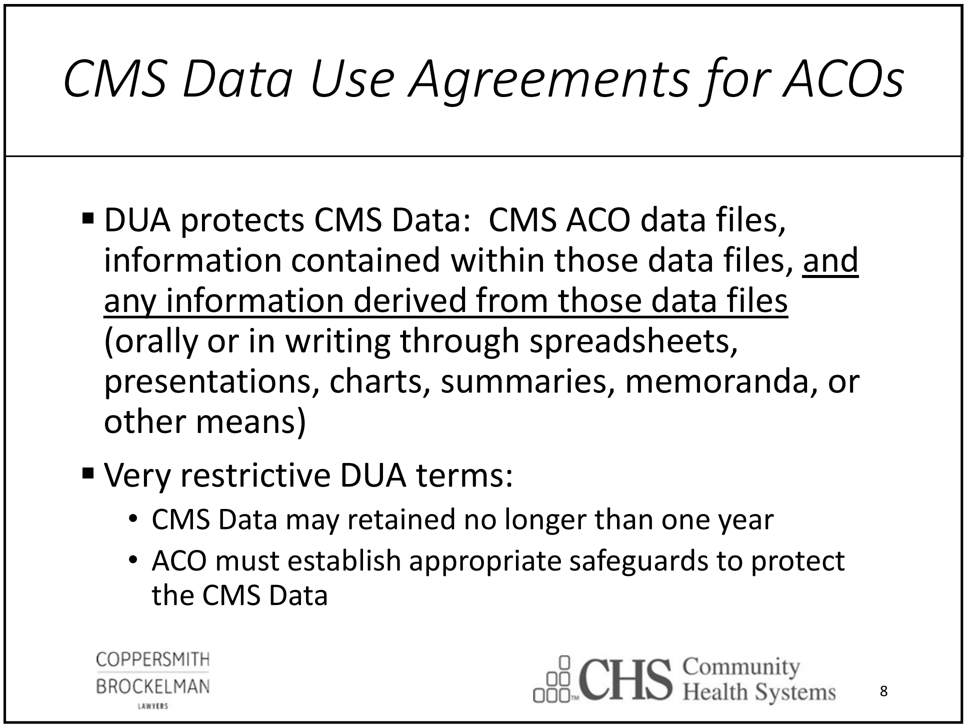
# HIPAA Compliance: Challenges in Collaborative Care

- Payor access
  - OHCA not always feasible
  - Individual right to withhold PHI from health plans if individuals pay in full out-of-pocket for service (even if participate in an OHCA)
- Minimum necessary standard
- Breach reporting obligations



# Part 2 Compliance

- Data protected under Part 2: (i) identifies a patient has having (or having had) a substance use disorder; and (ii) was obtained or generated by a "federally assisted" substance use disorder "program"
- Applies to: (i) Part 2 programs; (ii) qualified service organizations (QSOs) and their downstream contractors; (iii) health plans; and (iv) others that receive Part 2 data with consent and a re-disclosure notice
- Access to Part 2 data <u>very</u> limited
  - Consent required to access for treatment (unless emergency)
  - Consent required to access for care coordination/case management
  - Consent required to access for HCO (unless recipient is QSO)
- Challenges
  - Consent requirements difficult to meet
  - Data segregation is often not possible within EHRs



# CMS Data Use Agreements for ACOs

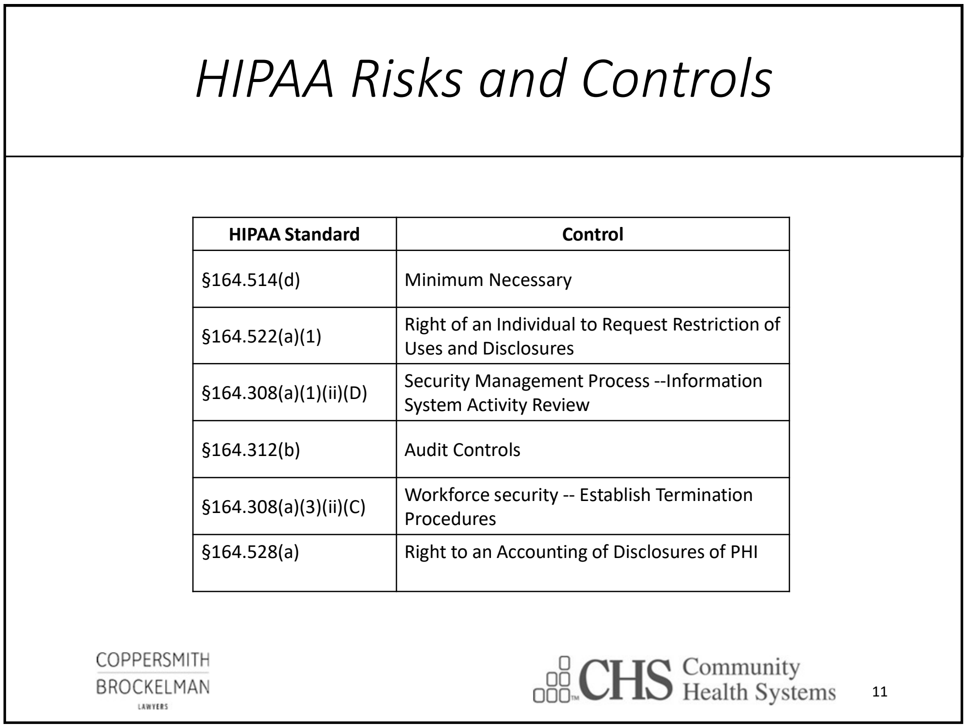
- DUA protects CMS Data: CMS ACO data files, information contained within those data files, <u>and any information derived from those data files</u> (orally or in writing through spreadsheets, presentations, charts, summaries, memoranda, or other means)
- Very restrictive DUA terms:
  - CMS Data may retained no longer than one year
  - ACO must establish appropriate safeguards to protect the CMS Data

# CMS Data Use Agreements for ACOs

- Very restrictive DUA terms continued…
  - Access to CMS Data only by the ACO, ACO Participants, and third parties that have signed a CMS Data Use Agreement
  - Access only by authorized individuals with a specific need to access CMS Data for ACO purposes (e.g. clinical treatment, care management and coordination, quality improvement activities, and provider incentive design and implementation)
  - Access only to the minimum necessary amount of CMS Data to meet the purpose of the request
  - If there is an external disclosure or misuse of the CMS Data, the ACO must alert CMS within ONE HOUR of the disclosure

# State Laws

- Changing landscape of state privacy laws – the California Consumer Privacy Act (CCPA) is a taste of things to come
- State health information confidentiality laws typically impose greater restrictions on use and disclosure of mental health information, HIV/communicable disease information, and genetic information
- Variation from state to state poses real challenges to sharing data within collaborative care arrangements that span state lines

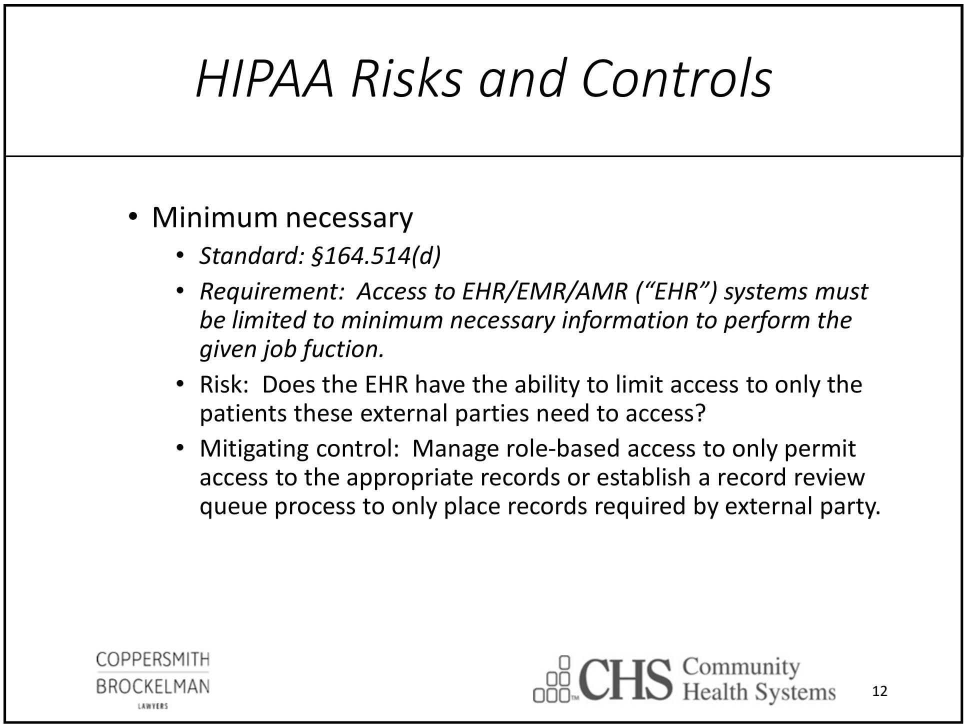


# HIPAA Risks and Controls

| HIPAA Standard | Control |
|---|---|
| §164.514(d) | Minimum Necessary |
| §164.522(a)(1) | Right of an Individual to Request Restriction of Uses and Disclosures |
| §164.308(a)(1)(ii)(D) | Security Management Process --Information System Activity Review |
| §164.312(b) | Audit Controls |
| §164.308(a)(3)(ii)(C) | Workforce security -- Establish Termination Procedures |
| §164.528(a) | Right to an Accounting of Disclosures of PHI |

COPPERSMITH BROCKELMAN LAWYERS

CHS Community Health Systems

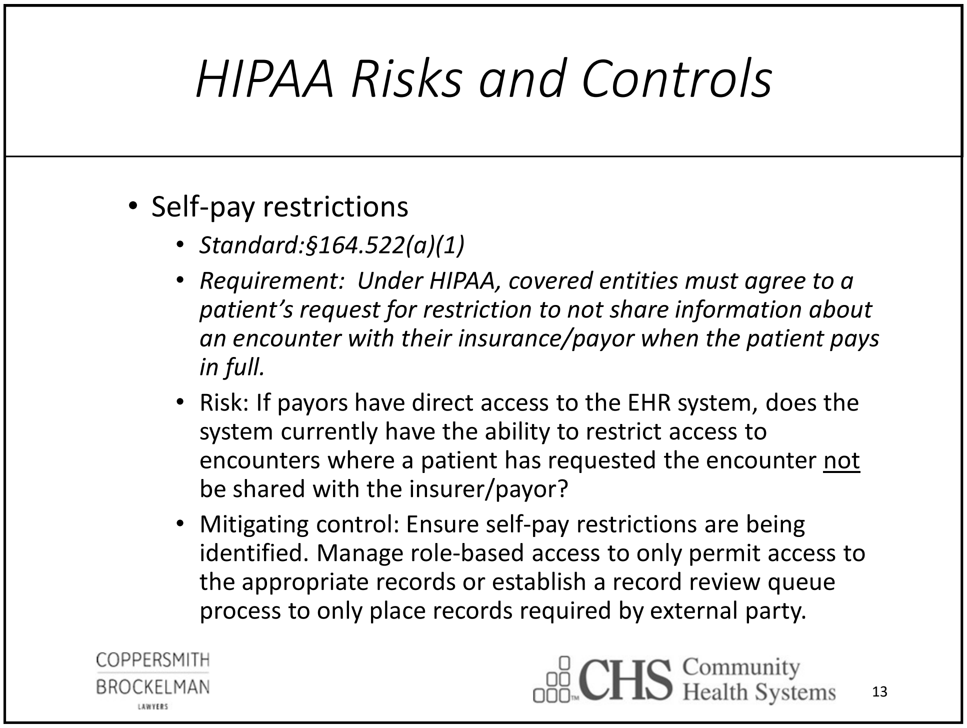


# HIPAA Risks and Controls

- Minimum necessary
  - *Standard: §164.514(d)*
  - *Requirement: Access to EHR/EMR/AMR ("EHR") systems must be limited to minimum necessary information to perform the given job fuction.*
  - Risk: Does the EHR have the ability to limit access to only the patients these external parties need to access?
  - Mitigating control: Manage role-based access to only permit access to the appropriate records or establish a record review queue process to only place records required by external party.

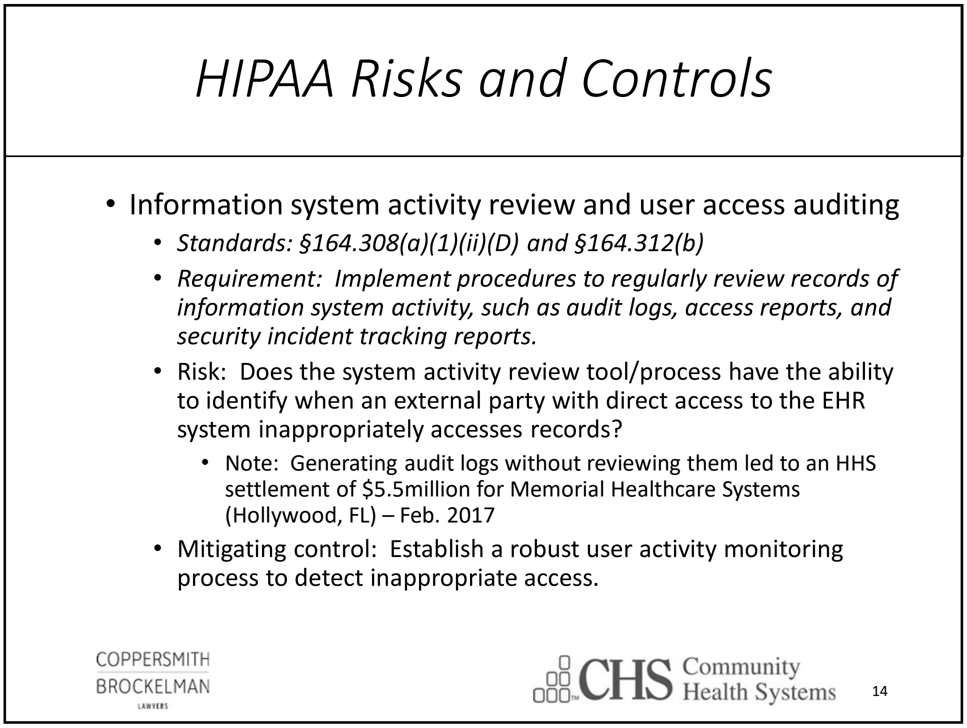
COPPERSMITH BROCKELMAN LAWYERS

CHS Community Health Systems



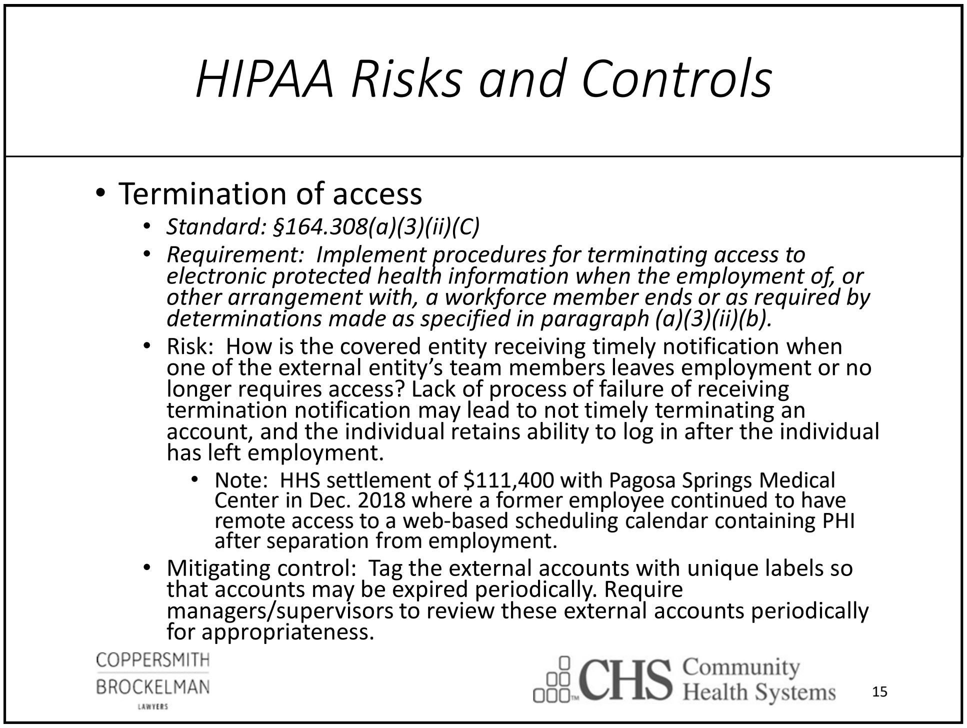
# HIPAA Risks and Controls

- Self-pay restrictions
  - *Standard:§164.522(a)(1)*
  - *Requirement: Under HIPAA, covered entities must agree to a patient's request for restriction to not share information about an encounter with their insurance/payor when the patient pays in full.*
  - Risk: If payors have direct access to the EHR system, does the system currently have the ability to restrict access to encounters where a patient has requested the encounter not be shared with the insurer/payor?
  - Mitigating control: Ensure self-pay restrictions are being identified. Manage role-based access to only permit access to the appropriate records or establish a record review queue process to only place records required by external party.



# HIPAA Risks and Controls

- Information system activity review and user access auditing
  - *Standards: §164.308(a)(1)(ii)(D) and §164.312(b)*
  - *Requirement: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
  - Risk: Does the system activity review tool/process have the ability to identify when an external party with direct access to the EHR system inappropriately accesses records?
    - Note: Generating audit logs without reviewing them led to an HHS settlement of $5.5million for Memorial Healthcare Systems (Hollywood, FL) – Feb. 2017
  - Mitigating control: Establish a robust user activity monitoring process to detect inappropriate access.



# *HIPAA Risks and Controls*

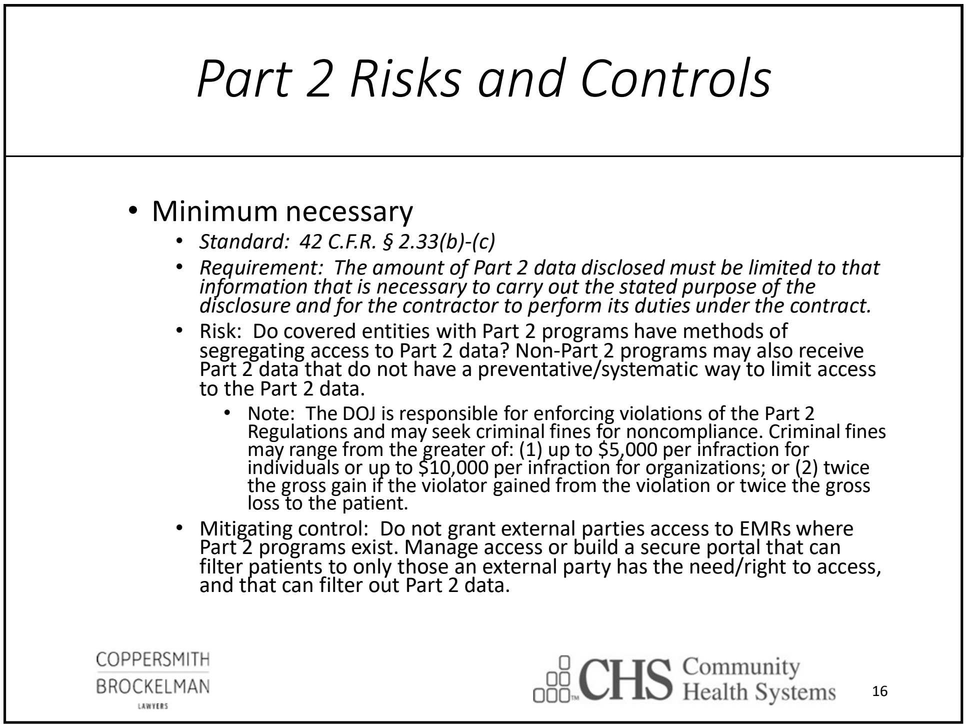
- Termination of access
  - *Standard: §164.308(a)(3)(ii)(C)*
  - *Requirement: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).*
  - Risk: How is the covered entity receiving timely notification when one of the external entity's team members leaves employment or no longer requires access? Lack of process of failure of receiving termination notification may lead to not timely terminating an account, and the individual retains ability to log in after the individual has left employment.
    - Note: HHS settlement of $111,400 with Pagosa Springs Medical Center in Dec. 2018 where a former employee continued to have remote access to a web-based scheduling calendar containing PHI after separation from employment.
  - Mitigating control: Tag the external accounts with unique labels so that accounts may be expired periodically. Require managers/supervisors to review these external accounts periodically for appropriateness.

COPPERSMITH BROCKELMAN LAWYERS

CHS Community Health Systems

15

15



# *Part 2 Risks and Controls*

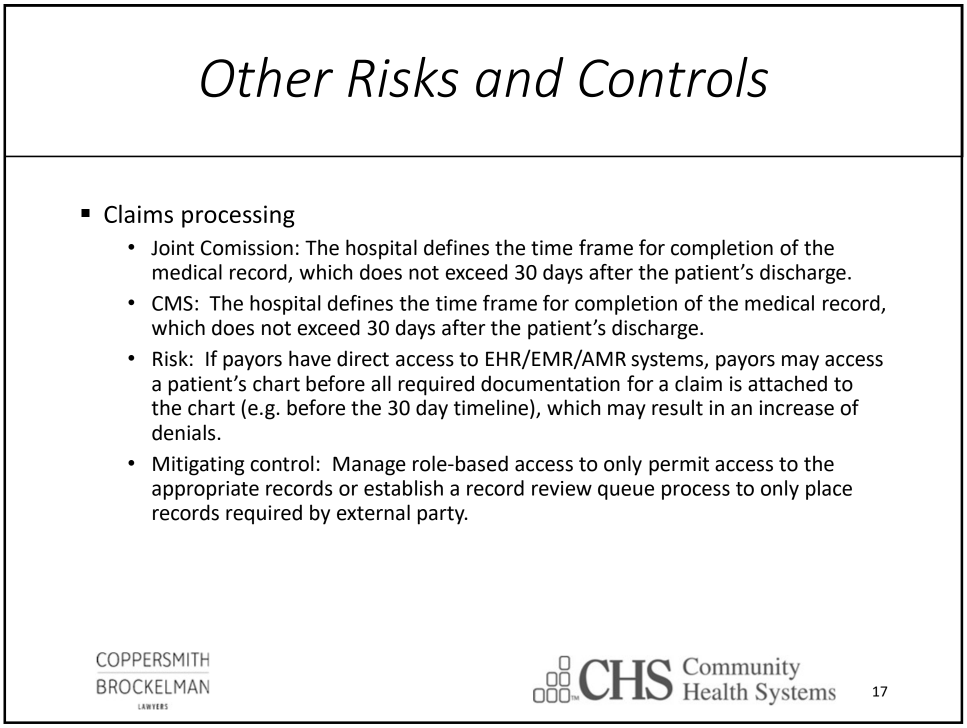
- Minimum necessary
  - *Standard: 42 C.F.R. § 2.33(b)-(c)*
  - *Requirement: The amount of Part 2 data disclosed must be limited to that information that is necessary to carry out the stated purpose of the disclosure and for the contractor to perform its duties under the contract.*
  - Risk: Do covered entities with Part 2 programs have methods of segregating access to Part 2 data? Non-Part 2 programs may also receive Part 2 data that do not have a preventative/systematic way to limit access to the Part 2 data.
    - Note: The DOJ is responsible for enforcing violations of the Part 2 Regulations and may seek criminal fines for noncompliance. Criminal fines may range from the greater of: (1) up to $5,000 per infraction for individuals or up to $10,000 per infraction for organizations; or (2) twice the gross gain if the violator gained from the violation or twice the gross loss to the patient.
  - Mitigating control: Do not grant external parties access to EMRs where Part 2 programs exist. Manage access or build a secure portal that can filter patients to only those an external party has the need/right to access, and that can filter out Part 2 data.

COPPERSMITH BROCKELMAN LAWYERS

CHS Community Health Systems

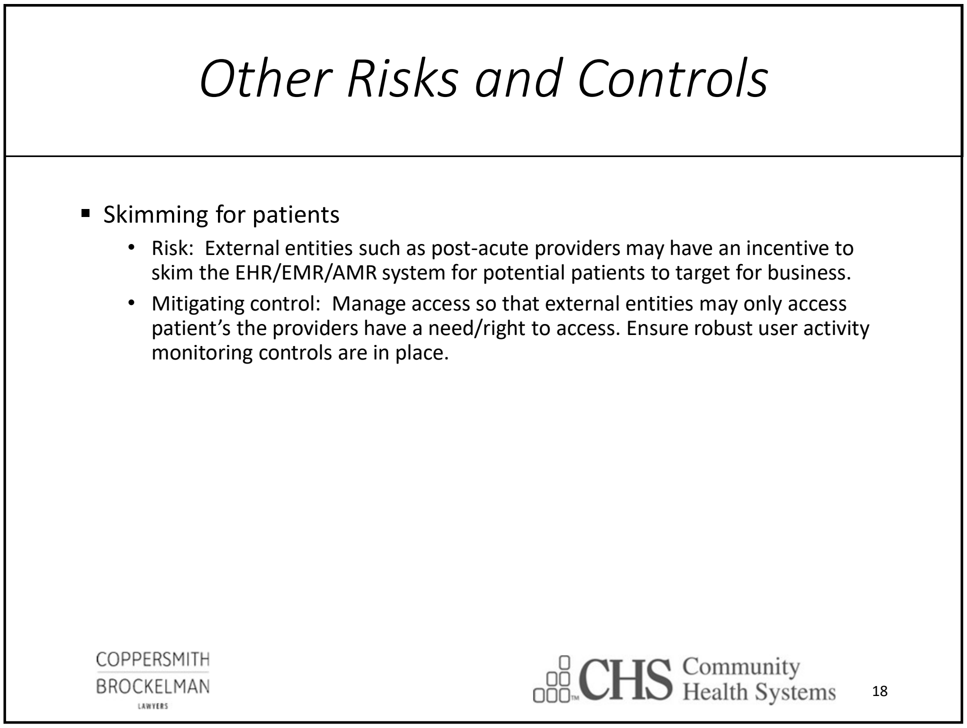
16

16



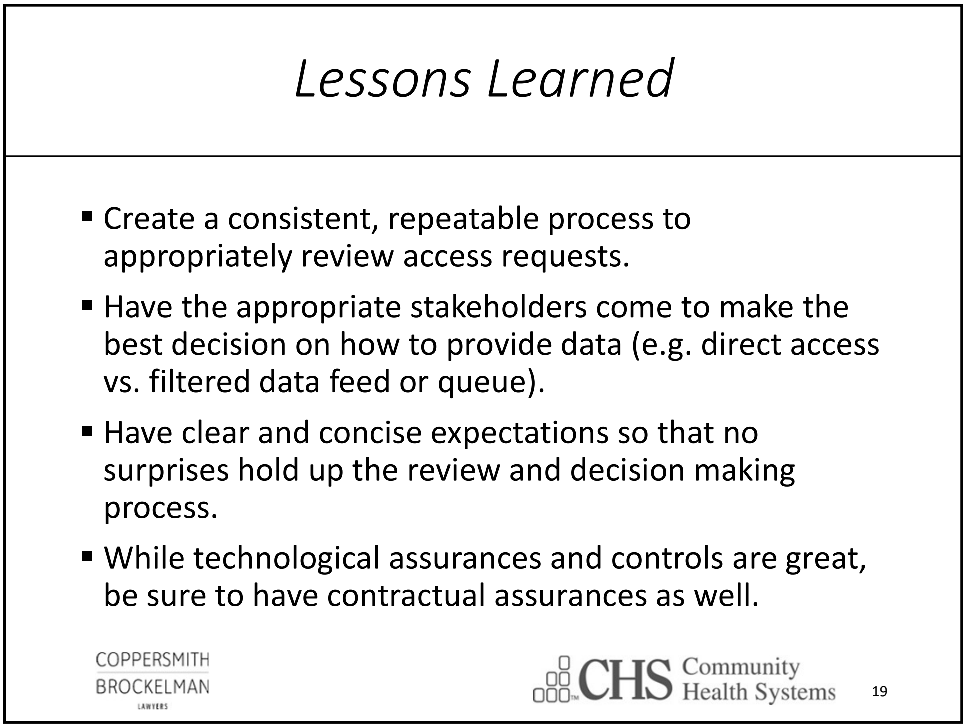
# Other Risks and Controls

- Claims processing
  - Joint Comission: The hospital defines the time frame for completion of the medical record, which does not exceed 30 days after the patient's discharge.
  - CMS: The hospital defines the time frame for completion of the medical record, which does not exceed 30 days after the patient's discharge.
  - Risk: If payors have direct access to EHR/EMR/AMR systems, payors may access a patient's chart before all required documentation for a claim is attached to the chart (e.g. before the 30 day timeline), which may result in an increase of denials.
  - Mitigating control: Manage role-based access to only permit access to the appropriate records or establish a record review queue process to only place records required by external party.



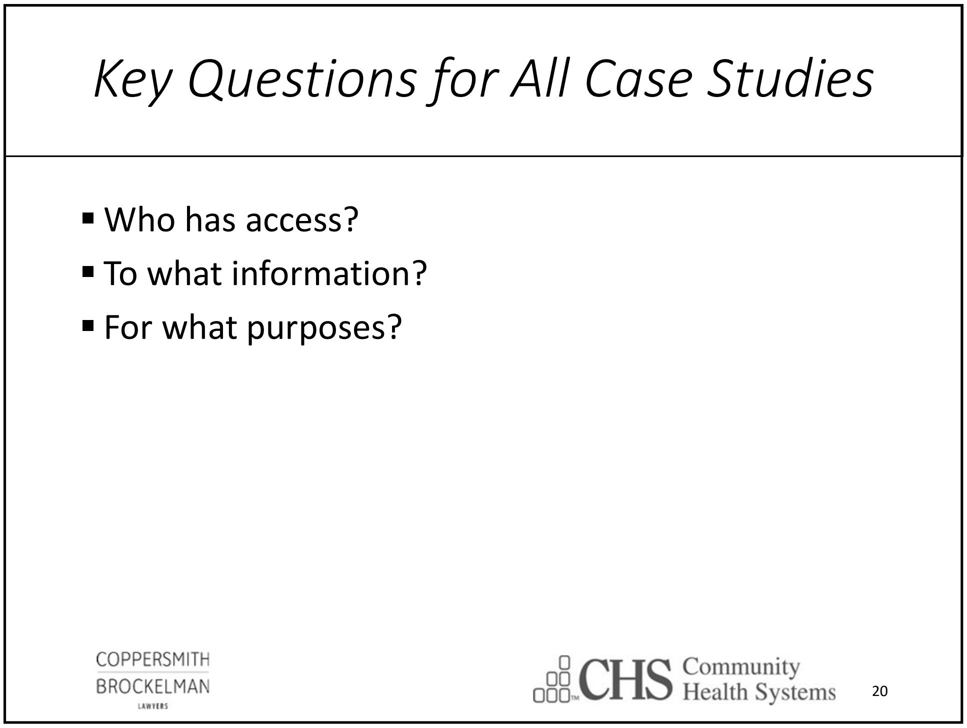
# Other Risks and Controls

- Skimming for patients
  - Risk: External entities such as post-acute providers may have an incentive to skim the EHR/EMR/AMR system for potential patients to target for business.
  - Mitigating control: Manage access so that external entities may only access patient's the providers have a need/right to access. Ensure robust user activity monitoring controls are in place.



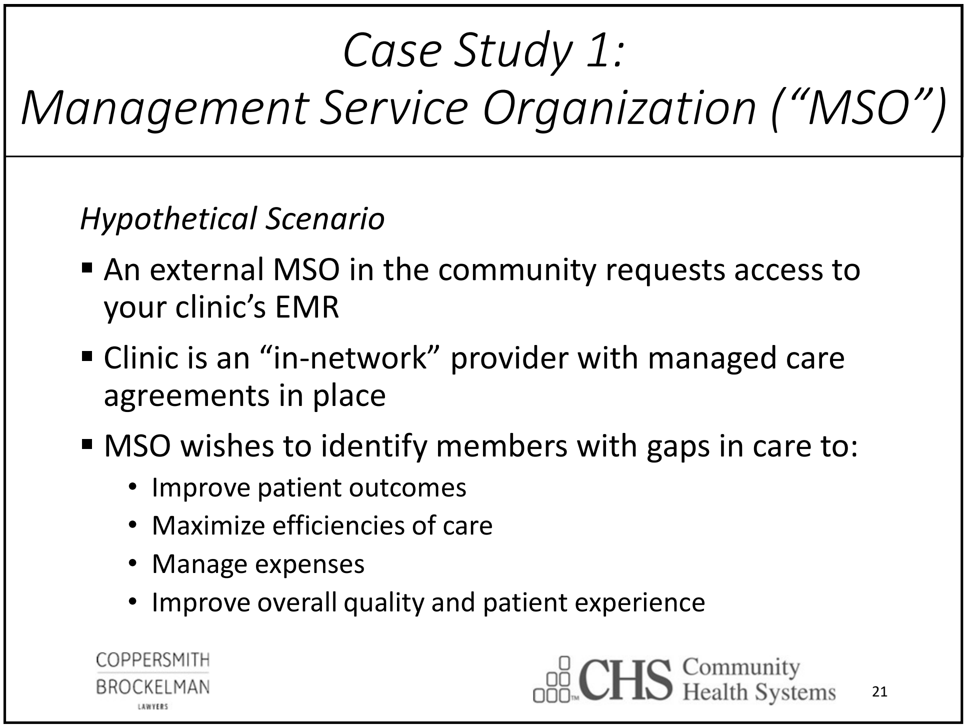
# *Lessons Learned*

- Create a consistent, repeatable process to appropriately review access requests.
- Have the appropriate stakeholders come to make the best decision on how to provide data (e.g. direct access vs. filtered data feed or queue).
- Have clear and concise expectations so that no surprises hold up the review and decision making process.
- While technological assurances and controls are great, be sure to have contractual assurances as well.



# *Key Questions for All Case Studies*

- Who has access?
- To what information?
- For what purposes?



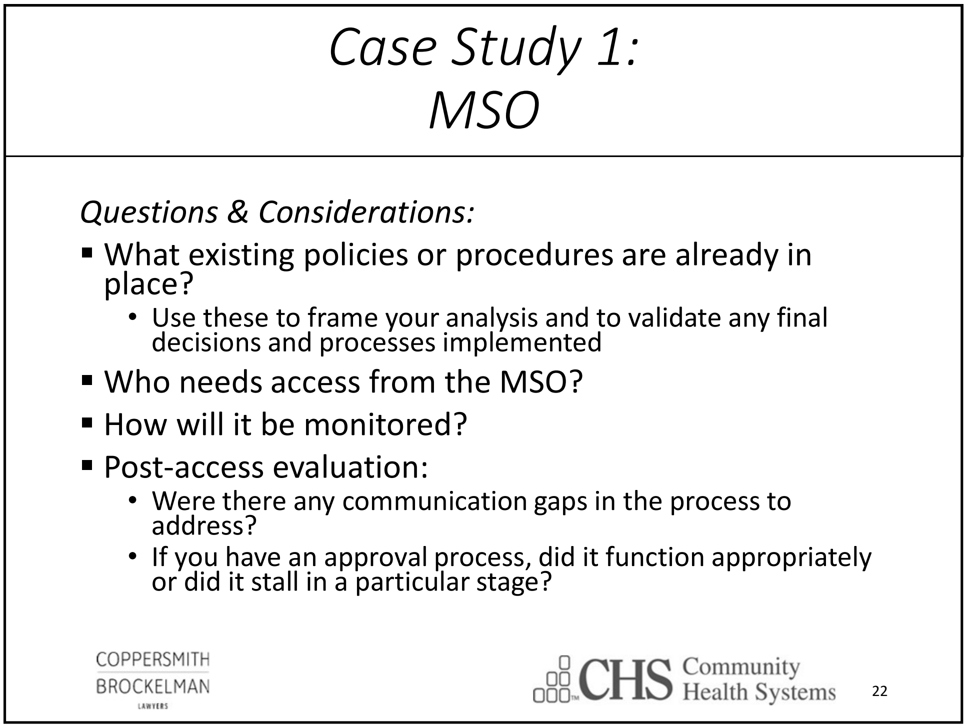
# Case Study 1: Management Service Organization (“MSO”)

*Hypothetical Scenario*

- An external MSO in the community requests access to your clinic’s EMR
- Clinic is an “in-network” provider with managed care agreements in place
- MSO wishes to identify members with gaps in care to:
  - Improve patient outcomes
  - Maximize efficiencies of care
  - Manage expenses
  - Improve overall quality and patient experience

COPPERSMITH BROCKELMAN LAWYERS

CHS Community Health Systems



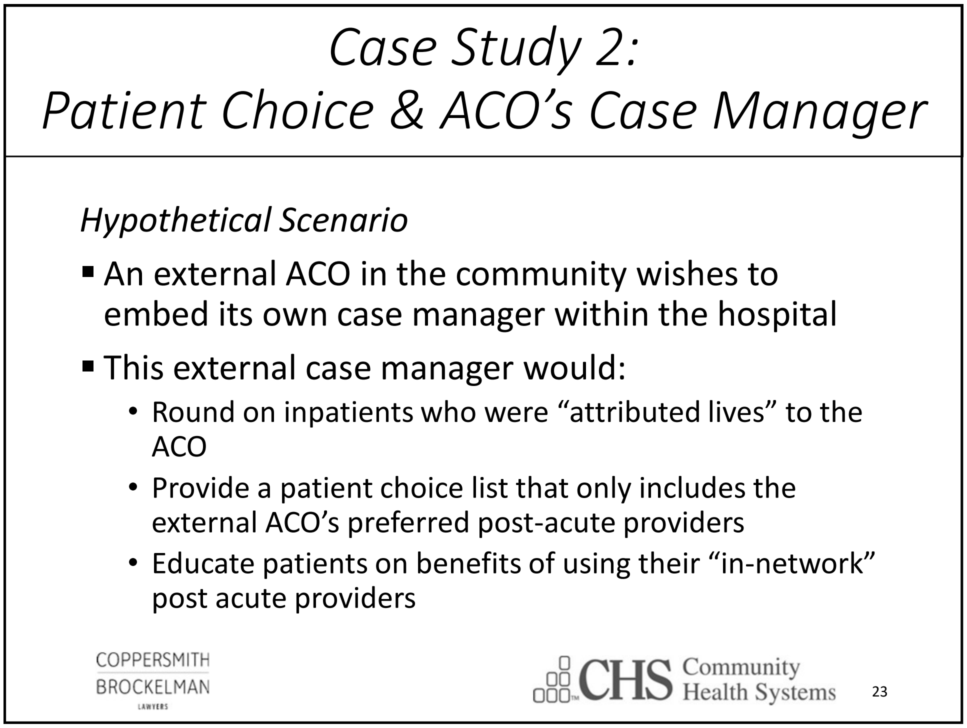
# Case Study 1: MSO

*Questions & Considerations:*

- What existing policies or procedures are already in place?
  - Use these to frame your analysis and to validate any final decisions and processes implemented
- Who needs access from the MSO?
- How will it be monitored?
- Post-access evaluation:
  - Were there any communication gaps in the process to address?
  - If you have an approval process, did it function appropriately or did it stall in a particular stage?

COPPERSMITH BROCKELMAN LAWYERS

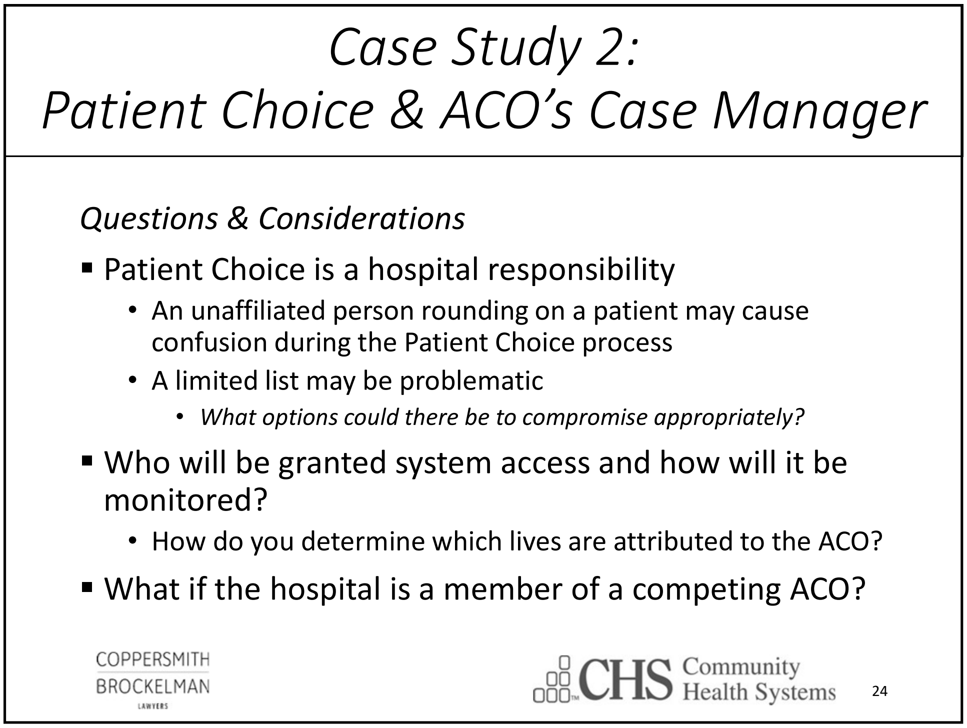
CHS Community Health Systems



# *Case Study 2: Patient Choice & ACO's Case Manager*

*Hypothetical Scenario*

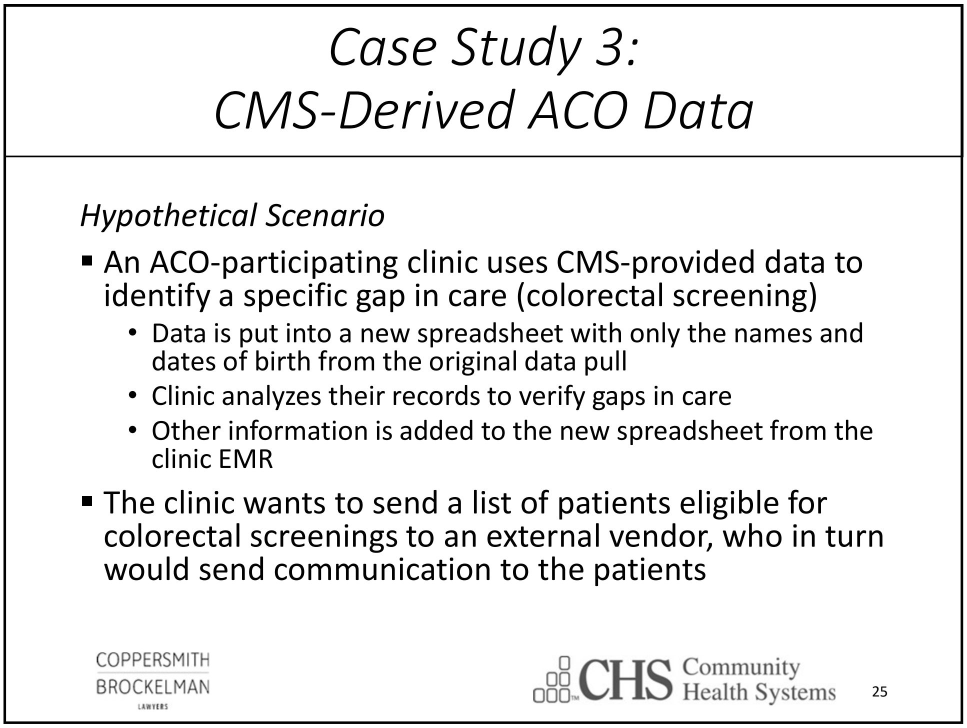
- An external ACO in the community wishes to embed its own case manager within the hospital
- This external case manager would:
  - Round on inpatients who were "attributed lives" to the ACO
  - Provide a patient choice list that only includes the external ACO's preferred post-acute providers
  - Educate patients on benefits of using their "in-network" post acute providers



# *Case Study 2: Patient Choice & ACO's Case Manager*

*Questions & Considerations*

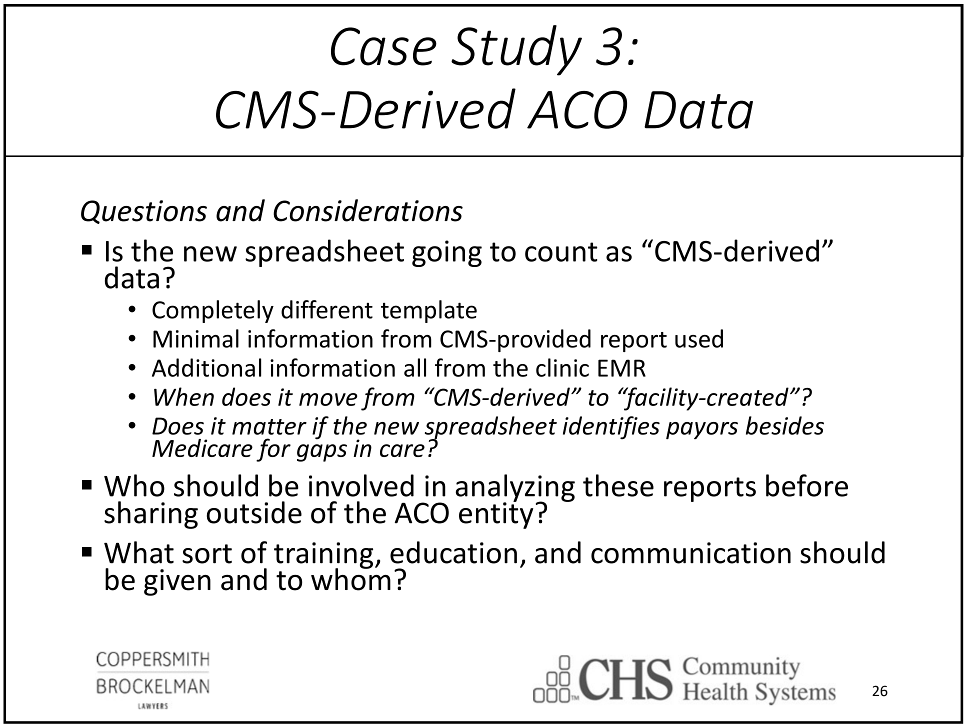
- Patient Choice is a hospital responsibility
  - An unaffiliated person rounding on a patient may cause confusion during the Patient Choice process
  - A limited list may be problematic
    - *What options could there be to compromise appropriately?*
- Who will be granted system access and how will it be monitored?
  - How do you determine which lives are attributed to the ACO?
- What if the hospital is a member of a competing ACO?



# *Case Study 3: CMS-Derived ACO Data*

*Hypothetical Scenario*

- An ACO-participating clinic uses CMS-provided data to identify a specific gap in care (colorectal screening)
  - Data is put into a new spreadsheet with only the names and dates of birth from the original data pull
  - Clinic analyzes their records to verify gaps in care
  - Other information is added to the new spreadsheet from the clinic EMR
- The clinic wants to send a list of patients eligible for colorectal screenings to an external vendor, who in turn would send communication to the patients



# *Case Study 3: CMS-Derived ACO Data*

*Questions and Considerations*

- Is the new spreadsheet going to count as “CMS-derived” data?
  - Completely different template
  - Minimal information from CMS-provided report used
  - Additional information all from the clinic EMR
  - *When does it move from “CMS-derived” to “facility-created”?*
  - *Does it matter if the new spreadsheet identifies payors besides Medicare for gaps in care?*
- Who should be involved in analyzing these reports before sharing outside of the ACO entity?
- What sort of training, education, and communication should be given and to whom?

COPPERSMITH
BROCKELMAN
LAWYERS

CHS Community
Health Systems

Kristen B. Rosati
Coppersmith Brockelman PLC
krosati@cblawyers.com
602-381-5464

Tyler Golden
CHSPSC, LLC
tyler_golden@chs.net
615-786-8142

Heathyr Fields
CHSPSC, LLC
heathyr_fields@chs.net
615-465-7292

27