Click here for audio.

AGENDA
Accountable Care Organizations Bootcamp Webinar Series, Part III: HIT and Data Sharing Issues for the ACO

March 28, 2013

1:00-1:05 pm	**Alisa L. Chestler, Esquire** Of Counsel Baker Donelson Bearman Caladwell & Berkowitz PC Washington, DC	Introduction
1:05-1:30 pm	**Heather L. Fields, Esquire** Shareholder Reinhart Boerner Milwaukee, WI	Overview of ACOs and HIPAA
1:30-1:55 pm	**M. Daria Niewenhous, Esquire** Member Mintz Levin Cohn Ferris Glovsky & Popeo PC Boston, MATB	Vendor Relationships and Security Issues
1:55-2:15 pm	**Amy S. Leopard, Esquire** Partner Bradley Arant Boult Cummings LLP Nashville, TN	ACOs and Data Sharing Agreements
2:15-2:30 pm	All	Q & A

AHLA

Accountable Care Organizations Bootcamp Webinar Series, Part III: HIT and Data Sharing Issues for the ACO

This webinar is brought to you by the Accountable Care Organization Task Force (a joint endeavor of all sixteen AHLA Practice Groups).

March 28, 2010

Presenters

Heather L. Fields, Esquire,
Shareholder, Reinhart Boerner Van Deuren s.c., Milwaukee, WI, hfields@reinhartlaw.com

Amy S. Leopard, Esquire,
Partner, Bradley Arant Boult Cummings LLP, Nashville, TN, aleopard@babc.com

M. Daria Niewenhous, Esquire,
Member, Mintz Levin Cohn Ferris Glovsky & Popeo PC, Boston, MA, DNiewenhous@mintz.com

Moderator

Alisa L. Chestler, Esquire,
Of Counsel, Baker Donelson Bearman Caladwell & Berkowitz PC, Washington, DC, achestler@bakerdonelson.com

AHLA

Overview of ACOs and HIPAA

Heather L. Fields
Reinhart Boerner Van Deuren s.c.
Milwaukee, WI
hfields@reinhartlaw.com

AHLA

Key Concepts

- Types of PHI ACOs Need
- ACOs and HIPAA Designation (CE, ACE, BA)
- Application of Select Privacy Requirements to ACOs
- HIPAA Security and ACOs
- State Law

AHLA

ACOs and PHI

- CMS Four Data Elements – 42 CFR § 425.702(c)
  - Name
  - DOB
  - Sex
  - Health Insurance Claim Number
- Claims Data
- Clinical Outcomes
- Utilization/Population Metrics

AHLA

ACOs and HIPAA Designation

- HIPAA and ACO Structures
  - "Closed System" ACOs vs. Multi-party ACOs
- Absent establishment of arrangement among Covered Entities, such as OHCA or ACE, Covered Entities need to consider:
  - Sharing and Opt-Out Agreements - 42 C.F.R. §425.708
  - Individual Privacy Officers
  - Individual Notices of Privacy Practices
  - Specific limits of Consent and Disclosure

AHLA

ACOs and HIPAA Designation (cont.)

- HIPAA "Designation" Options
  - Affiliated Covered Entity (ACE)
  - Organized Health Care Arrangement (OHCA)
  - Business Associate (BA)
- Implications
  - PHI Use/disclosure requirements
  - HIPAA compliance requirements
  - Other

AHLA

OHCA Refresher

- CEs that need to share PHI about patients to manage and benefit a common enterprise (45 CFR § 160.103)
- Clinically integrated care setting involving patient care by more than one provider
- Organized system of health care (more than one covered entity) **holding itself out** as joint arrangement participating in UR, QA or payment.

AHLA

Affiliated Covered Entities Refresher

- Common ownership or control
- **MUST** produce single NPP (45 CFR § 164.504(d)) – compare with OHCAs (permissive)
- May have BAAs *among* entities within an ACE
- TPO **uses and disclosures** are permitted without consent or authorization
- Joint and several liability?
- Note: if ACE combines functions of plan or provider, ACE may use or disclose PHI of patients only if patient receives **both** plan or provider services

AHLA

Comparison of Select HIPAA Compliance Requirements

	OHCA	ACE	BA
Privacy Officer	Single privacy officer	Single privacy officer	May not be needed?
NPPs	Optional joint notice	Mandatory single notice	No NPP
Use/Disclosure of PHI	Use/disclose PHI by/among OHCA members for TPO	If single NPP, use/disclose PHI by/among ACE members for TPO Plan/provider arrangement: only if individual receives benefits from both plan and provider	Use/disclose PHI only as provided in BAA
BAAs	No BAA needed Can use common BAA for vendor	No BAA needed Can use common BAA for vendor	Need BAA with each CE

AHLA

Select ACO HIPAA Privacy Considerations

- Minimum Necessary Rule
- Breach Notification
- Notice of Privacy Practices
- Individual Rights

AHLA

Minimum Necessary

- Use/Disclosure of PHI for payment and health care operations subject to minimum necessary requirements at 45 C.F.R. § 164.514(d)(1)
- Default for minimum necessary is limited data set if practicable per HITECH (42 USC § 17935(b)(1)(A))
- Required to be consistent with CE's minimum necessary policies and procedures? See 78 Fed. Reg. 5599

AHLA

Breach Notification

- **Interim Final Rule**: No disclosure required unless significant risk of "financial, reputational, or other harm to the individual"
- **Omnibus Rule**: Presumption of breach unless Covered Entity (CE) or Business Associate (BA) demonstrates, through a formal risk assessment, that there is a "low probability" that the Protected Health Information (PHI) was compromised
  - Includes limited data sets and minimum necessary violations

AHLA

Breach Notification

- Who gets notified?
  - Who notifies whom?
  - When is notification required?
  - How must the notification be given?
- Breach notification protocols/procedures for ACO participants?
- Other contractual obligations?
- Indemnity and insurance considerations

AHLA

Notice of Privacy Practices

- Helpful to describe ACO "practices"?
- Include opt-out procedures in NPP?
  - For MSSP, must provide "meaningful opportunity" for beneficiary to opt out of sharing 42 C.F.R. § 425.704.
    - Can be done through standard written notice (30 day rule) 42 C.F.R. § 425.708(b)
    - Can also be at first primary care ACO visit 42 C.F.R. § 425.708(c)
  - Relevance for other non-MSSP ACO programs?
  - Effect of opt-out on PHI sharing?

AHLA

ACOs and Individual Rights: the Designated Record Set

- Individual rights obligations pertain to PHI in designated record set…. 45 C.F.R. § 164.501
  - Medical and billing records,
  - Enrollment, payment, claims adjudication, and case or medical management record systems, and
  - Any information used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the CE.
- Consider if ACO maintains any part of the designated record set?

AHLA

ACOs and Individual Rights: Accounting of Disclosures

- Privacy Rule provides patient right to request and receive accounting of all disclosures of PHI by CE in last 6 years, subject to exceptions for TPO disclosures.
- HITECH (§ 13405(c)) removes exceptions if disclosure made through electronic health record
- Under HITECH, CE could either provide accounting on its own or refer individual to BA for accounting w/r/t EHRs
- Additional considerations for ACOs?

AHLA

HIPAA Security Rule

- BAs must be fully compliant – consider ACO's HIPAA security compliance infrastructure
- Consider carefully appropriate allocation of HIPAA security among ACO participants - no OHCAs under Security Rule
- More later…..

AHLA

State Law/Special Protections for Sensitive PHI

- State confidentiality laws
  - Mental health and developmental disability confidentiality protections
  - AODA
  - HIV
  - Others
- State breach notification laws

AHLA

Vendor Relationships and Security Issues

M. Daria Niewenhous, Esq.
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
Boston, Massachusetts
dniewenhous@mintz.com

AHLA

IT Vendor Relationships

- Identification and Selection
- Qualifications
- Due Diligence
- Communications

AHLA

Identification of Vendors Who Have PHI and other Protected Information

- Who are your current vendors that access or hold PHI and other protected information?
- Selection of new vendors
  - Are there “go to” vendors in your area of specialty?
  - Is your vendor’s system compatible with existing systems?
  - Where to start?

AHLA

Getting to Know You

- Who is the Vendor
  - Stand-alone?
  - Part of a larger affiliation?
    - Does vendor contract to affiliates or others?
      - Hardware, software, maintenance, website links, electronic data interchange?
  - Offshoring
    - Some contracts prohibit provider from contracting with off shore entities
      - Government payor/provider agreements

AHLA

Qualifications

- Qualifications
  - Third party certification is a fact to consider, but understand what goes into the certification process
    - HITRUST Certification for Data Security and Protection of Private Patient Health
    - ISO 27001
    - The Office of the National Coordinator for Health Information Technology (ONC) Certification Program
      - Process ensures that Electronic Health Record (EHR) technologies meet the adopted standards and certification criteria to help providers and hospitals achieve Meaningful Use (MU) objectives and measures established by CMS

AHLA

Qualifications, cont'd.

- Third party audit – again, understand the audit process
  - SSAE 16
- Financial stability
  - Source of funds
  - Debt load

AHLA

Data Security Program Issues

- Goal – Develop a legally defensible security program
  - If there is a data security issue, you will be called to show that the information security processes and procedures were legally "reasonable" and met legal requirements
  - Communication
    - IT/security and legal counsel
  - Process – what is the rationale for choices?
    - The what and the why
  - Document the decision-making process

AHLA

Understand the Risk

- Identify and manage risk from the start
  - Risks
    - Vendor's systems
    - Vendor's security procedures and capabilities
    - Vendor's employees
    - Vendor's subcontractors
    - Vendor's finances
    - Vendor's disaster recovery plans
    - Vendor's initial and commitment to you as a customer

AHLA

Due Diligence

- Key Touchpoints for Information Security Due Diligence
  - Assess your capacity to conduct diligence – outsource if necessary
  - The application
    - list of hardware, software, development projects
    - understand the technology
    - provide vendor with sufficient information to help identify "fit" with existing and planned systems
  - Intellectual property
    - Who authored software?
    - Demonstrate right to use software/application
      - License agreements
      - Who "owns" work that employees/consultants develop?
      - Any challenges to IP?

AHLA

Due Diligence, cont'd

- Key Touchpoints for Information Security Due Diligence (cont'd)
  - Key relationships and contracts
  - Who are vendor’s largest customers?
  - Has vendor lost relationships over the past [3] years? Why?
  - Have vendor's customer's had data breaches?

AHLA

Where is My Data?

- Where, oh where, is my data?
  - Cloud?
  - Vendor's place of operations?
  - Outsourced?
  - Same state?
- Vendor's workspace
  - Safe & sound?
  - Security measures?
  - Is anybody home?

AHLA

Remote Access – Special Risks

- Laptops and remote access
  - Can employees “work from home”
    - On what equipment, remote access system?
  - Do employees use laptops?
    - Vendor's or their own?
      - Downloading policy?
    - Are mediaports/USB plus deactiviated?

AHLA

Subcontractor Access to Data

- Who has access to my data?
  - Will vendor's contractors have access to data?
    - In ordinary course
    - In unusual circumstance – maintenance
  - What diligence does vendor conduct on its contractors?
    - Initial and ongoing
    - Documentation
    - Corrective action to address deficiencies
- Does vendor hold its subcontractors to the standard you expect of the vendor?

AHLA

Vendor's Employees and Independent Contractors

- Who's working for the vendor?
  - Protocols for employee/independent contractor selection, screening, training
    - Frequency and content of screening, training
    - Confidentiality agreements? Noncompetes?
    - Qualifications for organizational/functional positions
  - Policies and procedures
    - Hire, employment, exit
      - Termination of user/access codes
      - Return/deactiviation of equipment, if applicable
  - Succession planning

AHLA

If Disaster Strikes

- Disaster Preparedness and Recovery
  - Physical operations/personnel
  - Back-up plans
    - Where is back-up located?
  - Testing protocols

AHLA

Risk – Protection and Shifting

- Insurance
  - List and copies of all policies
    - Cyberinsurance, business interruption, etc.
  - Has insurance been cancelled?
  - Claims history
- Indemnification

AHLA

Breach

- Breach response
  - Consider federal and state requirements
- Customer notification protocols

AHLA

Skeletons in the Closet?

- Investigation, litigation
  - Pending or threatened litigation
    - Private, governmental
  - Intellectual Property claims
  - Warranty claims
  - Requests for accounting of data
    - Customers
    - Patients/subject of data
  - Complaints – history, disposition, methodology for resolution
    - Customers
    - Patients/subjects

AHLA

How Much Diligence?

- How much diligence?
  - Assess risk – low, medium, high
  - Manage diligence to risk level
    - Documentation
    - Interviews
    - Site visit
    - Independent verification of controls
  - Risk can be identified, mitigated, but not eliminated
  - Talk to other customers
    - Not just those in the honeymoon period
    - Customers who ended the relationship

AHLA

Vendor Relationship

- Who is responsible for the account going forward?
  - Make sure the “A” Team is not just for sales
  - Compatibility with your team

AHLA

Vendor Contracts

- A whole other seminar!
- Have an expert review
  - Insurance
  - Indemnification
  - Breach response
  - Right to terminate
  - Right to amend
  - Notification to customer of issues
  - Verify controls/standards
    - Obligate Vendor to its current standards as a floor
    - Commitment to adapt standards as requirements evolve
    - Vendor subcontracts

AHLA

Vendor Contracts, cont'd

- Pricing
- Upgrades to vendor's system
- Data
  - Use, ownership, security
  - Risk of loss
  - Preserving/returning data
    - Who determines if data is returned or destroyed

AHLA

Vendor Contracts, cont'd.

- Cloud Vendor Contracts
  - Address:
    - Data Risk
    - Continuity of Services
    - Audit rights
    - Assignment
    - Location(s) of data

AHLA

Addenda

- Business Associate Agreements
- Data Use Agreements
- Minimum Security Standards
- Other?

AHLA

ACOs and Data Sharing Agreements

Amy S. Leopard, Esquire,
Partner
Bradley Arant Boult Cummings
aleopard@babc.com

AHLA

“I’ll have what she’s having . . . “

Data Use Agreements (DUAs) are multilateral agreements to manage information sharing by contract

AHLA

“I’ll have what she’s having . . . “

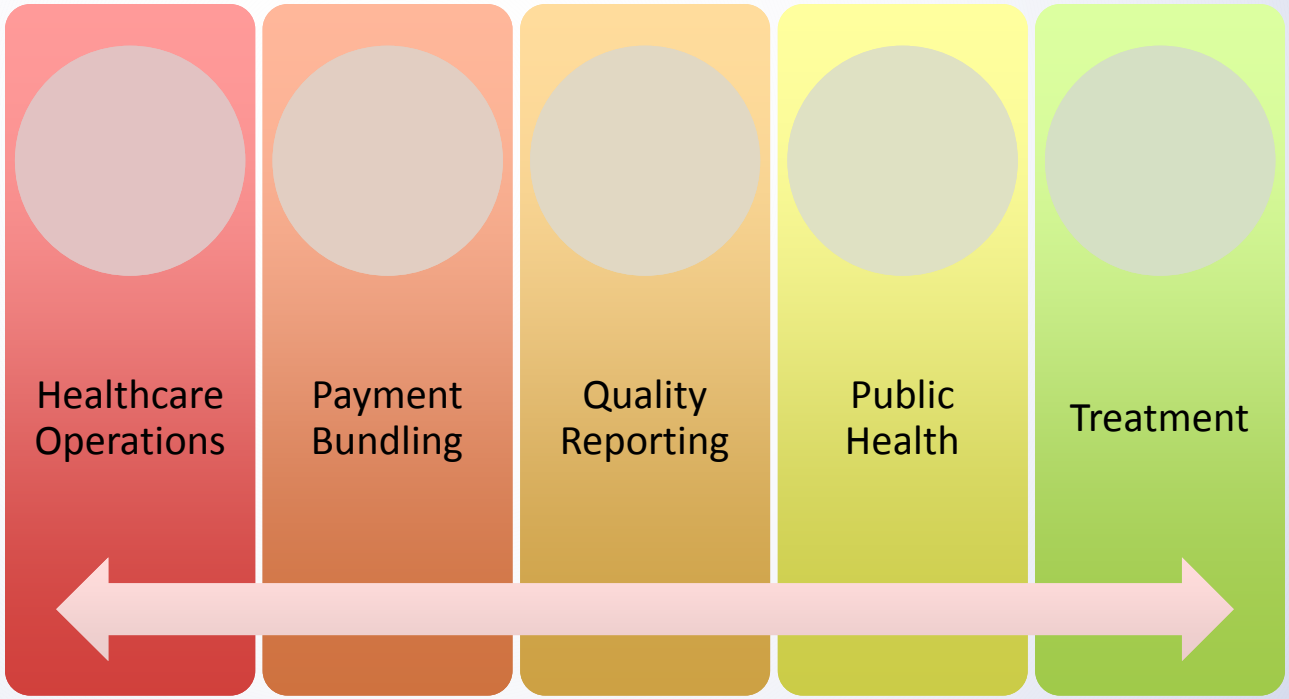
Data sharing and agreements inherently are driven by

- Objectives for data sharing
- Consent model
- Identified Participants
- Identified data
- Governance
- Flexibility

Data Use Agreements (DUAs) are multilateral agreements to manage information sharing by contract

AHLA

Objectives drive Data Sharing Agreement



- Is the purpose of data sharing to improve quality, evaluate providers, determine how to reimburse providers (e.g., bundled or encounter-based payments), report quality data to CMS or other payors, improve public health, or coordinate care across the continuum?

AHLA

MSSP Data Sharing *Objectives*

Internally Reporting on Quality and Cost Metrics	• Define, establish, implement, evaluate and periodically update its process and infrastructure to support internal reporting on quality and cost metrics • Monitor, provide feedback, and evaluate ACO participant and ACO provider/supplier performance and use results to continually improve care and service over time

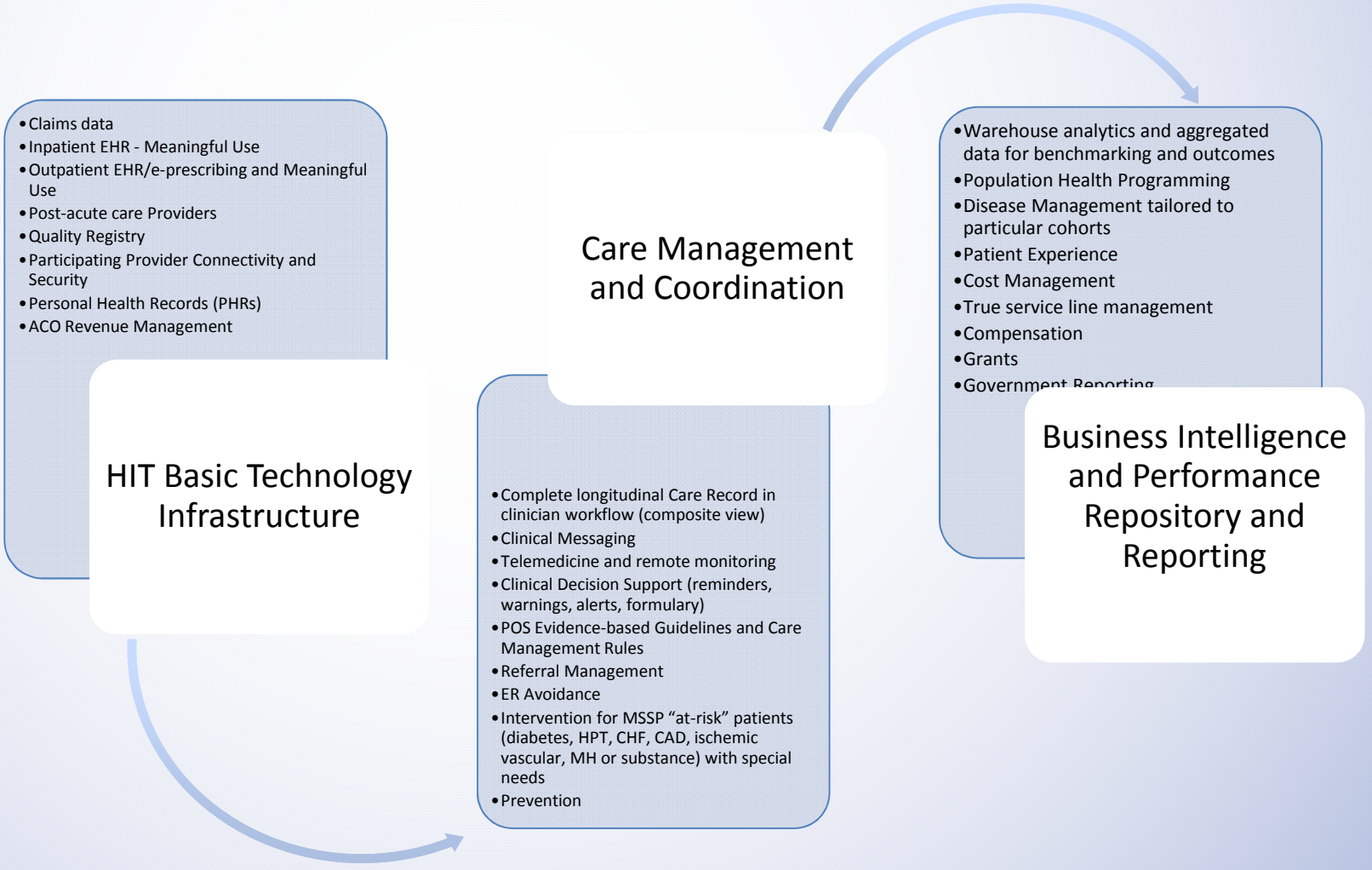
Promoting Coordination of Care	• Define, establish, implement, evaluate and periodically update care coordination processes
	  • Methods to coordinate through episode of care and transitions
	  • target populations that would benefit from individualized care plans and sample individual care plan to promote improved outcomes for high-risk and multiple chronic conditions and account for community resources

Clinical Processes and Patient Centeredness	• Quality Assurance and Improvement Program • Promoting Evidence-Based Medicine • Promoting Beneficiary Engagement • Internally Reporting on Quality and Cost Metrics • Promoting Coordination of Care
Quality Assurance and Improvement Program	• Health care professional responsible for ACO QA, including promoting evidence-based medicine, promoting beneficiary engagement, reporting internally on quality and cost metrics, and coordinating care • ACO remedial process and penalties for those who fail to comply • ACO internal assessments of processes to continuously improve the care practices
Promoting Evidence-Based Medicine	• ACO must define, establish, implement, evaluate, and periodically update its process to promote evidence-based medicine • Cover diagnoses with significant potential for ACO to achieve quality improvements

Promoting Beneficiary Engagement	• ACO to have process to promote patient engagement and address:
	  • Evaluating health needs of assigned population
	  • Communicating clinical knowledge/evidence-based medicine to beneficiaries
	  • Beneficiary engagement and shared decision-making to account for unique needs, preferences, values and priorities
	  • Written standards for beneficiary access and communication for beneficiaries for medical record access

AHLA

What data? How will it be organized?



ACO is a data intermediary and as a Covered Entity or Business Associate, must consider data flows

AHLA

Data Sharing with CMS

- MSSP Application:
  - How ACO intends to use data AND will ensure privacy and security
    - to evaluate performance of ACO participants and ACO providers/suppliers
    - to conduct quality assessment and improvement activities
    - to conduct population-based activities to improve health of assigned beneficiary population
- CMS Data Use Agreement
  - Form DUA
  - Addendum for MSSP ACO Subcontractors
- Reporting information to CMS
  - Quality Metrics and Meaningful Use

AHLA

CMS Data Sharing *FROM* CMS under MSSP

- CMS will share
  - aggregate data on ACO's population utilization and expenditures
    - Initially and quarterly and in conjunction with annual reconciliation
  - PHI with requesting ACOs under a Data Use Agreement (DUA)
- *Population List*: CMS reports of preliminary prospectively assigned Medicare beneficiary population when agreement begins, quarterly, and beginning of each performance year
  - Name, DOB, sex, and HICN of beneficiaries used to generate ACO's benchmark
- *Monthly Claims Data*: Part A, B and/or D claims data for enumerated purposes on request under a DUA for preliminary prospectively assigned Medicare beneficiaries receiving ACO's opt-out notice and opportunity to decline
  - ACO may contact beneficiaries from population list to notify of future data sharing and opportunity to opt out (or obtain at next encounter)
  - If no opt-out response received within 30 days, ACO may request claims data, but beneficiary must be provided opt out opportunity at first primary care service visit with ACO participant
- ACO must certify to CMS as a HIPAA covered entity or BA re: proper purpose and "minimum necessary" requested to conduct Health Care Operations under 45 CFR 164.501, para. 1 and 2

Even if beneficiary opts out, ACO Participants can still exchange PHI under HIPAA

AHLA

Consent Model or Stewardship Model?

Opt-in with Restrictions

- No data automatically in but patient has option to include all or some categories/data elements, specific providers, particular purposes

Opt-in

- No data automatically available, so patients express preference to be "all in" or out

Opt-out with exceptions

- Opt out in full or selectively exclude categories/data elements, limit exchange to particular providers, or limit exchange for particular purposes

Opt-out Model (CMS Data Sharing Model)

- all or some data automatically exchanged but patient opportunity to opt out in full

NO CONSENT

- But HIPAA TPO exception still applies (Treatment, Payment and Healthcare Operations)

Goldstein Rein, "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" (2010)

AHLA

Data Use Agreements within the ACO

- Establish rules of engagement in advance for ACO to facilitate decisions on ownership, privacy and security and help manage risk at ACO level
- Participant Agreement, Business Associate Agreement or DUA may address
  - EHR Adoption requirements
  - Privacy & Security under HIPAA
  - Peer Review Privileges, if applicable
  - Data Provider Obligations for data submission and integrity
  - Data Recipient Parameters
  - ACO proprietary ownership, access and protection of data, software, improvements, protocols, decision support
  - Risk Allocation

Even if beneficiary opts out, ACO Participants can still exchange PHI under HIPAA

AHLA

Participants and Their Obligations

- CMS MSSP Data sharing
- Data Providers, typically Covered Entities
  - Standardization and Standards for Data Provided
  - Data integrity
  - BA Agreement flow down from Data Provider?
- Authorized Data Users
  - MSSP/ACO/HIPAA/OHCA Permitted Purposes
    - Permitted and Prohibited Uses and Disclosures
    - Role-based Access
  - BA flow down to Subcontractors?
  - Breach Reporting
  - Vendor license restrictions

AHLA

ACO Obligations

- DUA CMS, BA Responsibilities under HIPAA
  - CMS DUA
    - 1 hour breach and prohibition on further disclosures
      - http://www.resdac.org/sites/resdac.org/files/DUA_SignatureAddendum.pdf)
  - HIPAA BA Relationships with Plans?
  - Subcontractor BA relationships
- Disclaimers
  - Practice of Medicine, incomplete or inaccurate data, patient care
- Reps and Warranties
  - As is?
- Risk Allocation
  - Limitations of Liability/ Insurance/ Indemnifications
- Compliance
  - ACOs cannot limit or restrict health information sharing among providers and suppliers within or outside the ACO

AHLA

Data Sharing Governance Policies and Procedures

- **Privacy Practices**
  - Individual privacy rights and consent model
  - Regulation of collection, uses and disclosures
  - Mitigation and reporting of violations of privacy practices/HIPAA

- **Security Management Process**
  - Authorization and control
  - Encryption
  - Professional and institutional identification and authentication
  - Audit trail and information system activity review
  - Security incident response, including reporting of security breach

- **Competitive Issues**

DUA can reference external documents that may change periodically

AHLA

Flexibility for the Future

- Patient Engagement?
- Changes in technology to manage consent?
- Treatment Uses?
- Accounting for Disclosures?
- Sensitive Data?

AHLA

Questions?

AHLA