Status Check On Health IT

CTHIMA
Annual Conference
September 17, 2017

Slides Prepared by
Jennifer L. Cox, J.D.
Cox & Osowiecki, LLC
Hartford, Connecticut

©2017 Cox & Osowiecki, LLC

The Future Of Healthcare And Health IT Are Not Entirely Clear

The Suspense From Washington, D.C. builds…

©2017 Cox & Osowiecki, LLC

Healthcare Reform Roadblock: President Trump Explains the Problem

"It's an unbelievably complex subject. Nobody knew that health care could be so complicated."

-Donald J. Trump, President of the United States

February 27, 2017

©2017 Cox & Osowiecki, LLC

Massive Budget Cuts Coming

- There appears to be limited interest in more funding for healthcare, at any level
- Patient care, HIT, quality, research projects are all facing huge cuts
- Unprecedented cuts to:
  - HIT infrastructure, AHRQ, NIH, ONC, OCR
- Medicaid cuts are coming, but it's hard to tell what the structure will look like, or how hard the impact will be, until a state budget is in place

©2017 Cox & Osowiecki, LLC

A Theme Emerges

Slow (or no) action.

©2017 Cox & Osowiecki, LLC

Slow Action On Repeal of PPACA

- No way to tell where this lands
- Many CO-OPs have already failed
- Exchanges could fail because insurance companies do not see enough ROI (if any ROI)
- Unclear how dedicated the government is to ACOs or Value-based purchasing

©2017 Cox & Osowiecki, LLC

Slow Action on 21st Century Cures Act

- 21st Century Cures Act meant to provide a roadmap for:
  - data sharing
    - Including API mandates
  - interoperability
  - information blocking rules
  - research guidance
- This *could* be the single biggest shift in access rules since HIPAA, but…**the Act needs rules and guidance before it can go into effect**

©2017 Cox & Osowiecki, LLC

21 Century Cures

- FDA, ONC and OCR (at a minimum) all need to come up with new rules, and not all the rules fit together well
- Guidance appears to be months behind schedule
- Now targeting Spring of 2018 for the 1st publicly available proposed set of rules
  - That's slow by any standard!!

©2017 Cox & Osowiecki, LLC

The Future of Meaningful Use

- **Medicare MU** is now only for hospitals
  - Eligible professionals who were doing Medicare MU will be transitioned to MACRA-MIPS, and follow Advancing Care Information reporting (watered down MU)
- **There is no Medicare MU program for EPs**
- Medicaid MU continues for both hospitals and EPs
- Secretary Tom Price and the administration are unlikely to support increased or new EHR incentive programs

©2017 Cox & Osowiecki, LLC

MACRA-MIPS: Who's In?

- Moving Target of Who qualifies for MACRA
- Last number was "up to 418,849" are expected to submit MIPS data – but that line may have moved
- CMS has already sent letters to 806,879 clinicians saying despite prior notices, they will not be evaluated under MIPS in 2017
- Exempt providers includes those:
  - Thresholds…less than $30,000 in Medicare charges (might move to $90,000); fewer than 100 unique Medicare patients per year (might move to 200 or more)
  - New to Medicare (exempt for this year)

©2017 Cox & Osowiecki, LLC

MACRA: Advancing Care Information

- ACI is 25% of the overall MACRA score
- Points are tallied based on segments of the ACI objectives
  - Required Objectives (5)
  - Optional Objectives (5 available, pick up to 4)
  - Bonus for Public Health Reporting (pick up to 5)

©2017 Cox & Osowiecki, LLC

Five Required ACI Objectives

- Requires 5 objectives to qualify for any points
  - Patient access rights met
  - Security Assessment performed
  - E-Prescribing
  - SEND summary of care
  - RECEIVE/RETRIEVE summary of care

©2017 Cox & Osowiecki, LLC

Five “Optional” ACI Objectives

Choose up to 4 of these 5 to add points (note: points can only be achieved if you complete the entire list of 5 required objectives)

- Secure messaging
- View-Download-Transmit
- Patient Specific Education
- Clinical Information Reconciliation
  - Med rec/allergy check/problem list review
- Accept Patient Generated Health Data

©2017 Cox & Osowiecki, LLC

MACRA Changes to Public Health Reporting 2017 (and Beyond)

- Public Health Reporting becomes (*mostly*) optional – in the "bonus" category
- PHR categories were expanded consistent with earlier MU Stage 3 guidance:
  - Immunization reporting to government program
  - Syndromic Surveillance
  - Specialized Registry/Case Registry
  - Electronic Lab Reporting
  - Public Health Registry
  - Clinical Data Registry

©2017 Cox & Osowiecki, LLC

Privacy Improvement For SSNs

- Federal government is removing Social Security Numbers from Medicare files and cards
- Medicare enrollees will be give a NEW number
- Project to supply new cards done by April 2019, with provider (and billing) compliance by December 2019

©2017 Cox & Osowiecki, LLC

What To Expect Next(?)

"You've got to be very careful if you don't know where you are going, because you might not get there."

-Yogi Berra

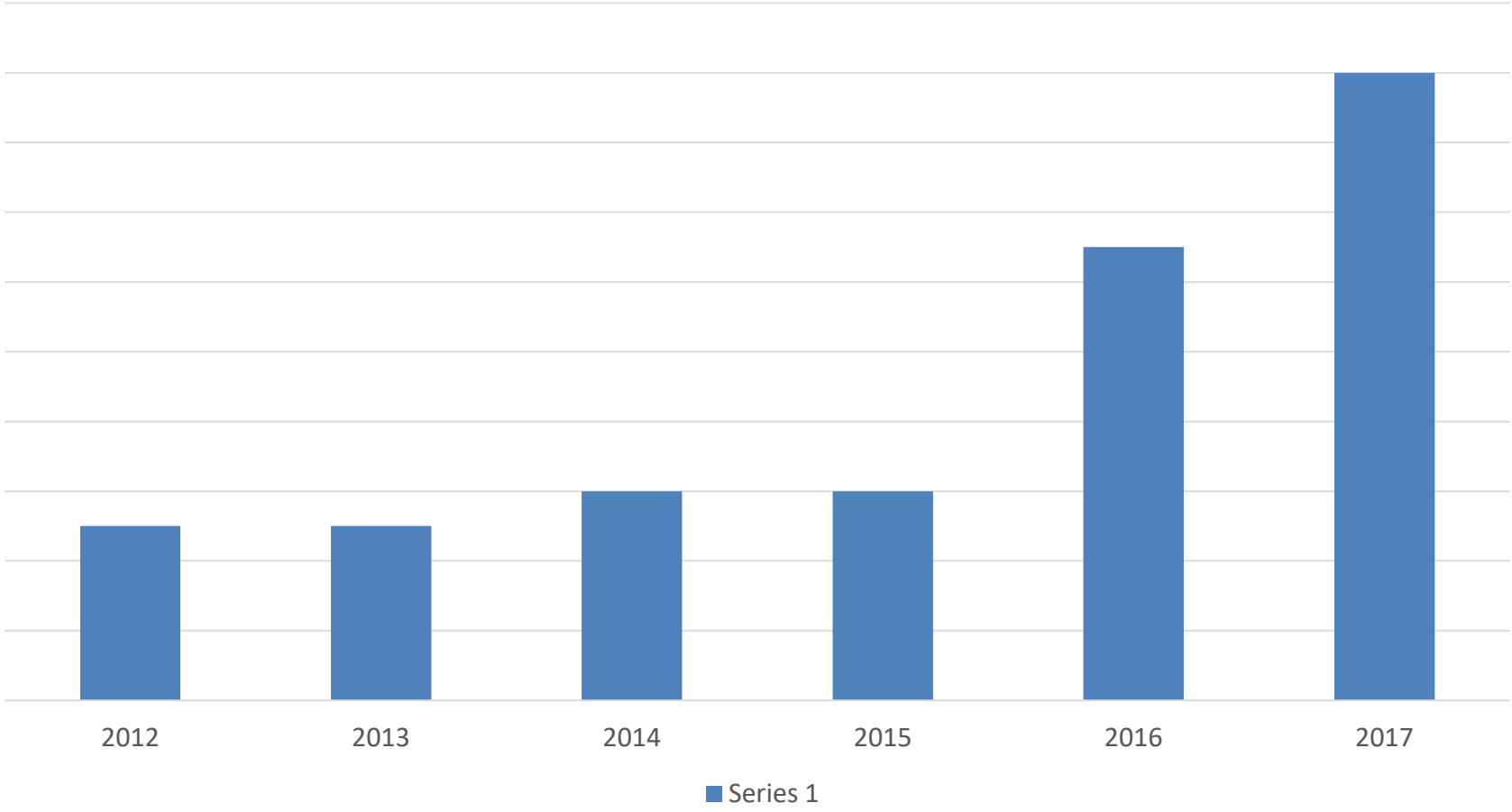
©2017 Cox & Osowiecki, LLC

HIPAA Rules: Increased OCR Enforcement

More settlements, higher “highs”

©2017 Cox & Osowiecki, LLC

A More Aggressive OCR Resolution Agreements Per Year



©2017 Cox & Osowiecki, LLC

HIPAA Resolution Agreements

The last year of data is impressive for the high value resolutions, and sheer volume.

But we see the same types of events occurring.

©2017 Cox & Osowiecki, LLC

Really – Don't Just Ignore HIPAA Rules

- **August 2016**, $5.5m penalty - Advocate Health Care (Illinois)
- Three sequential breaches reported in 2013 – over 4 million patients' PHI
- Multiple failures: insufficient policies, failure to perform security risk assessment, no physical safeguards, missing BAAs for vendors, unencrypted portable devices

Healthcare System Must Update BAAs

- **September 2016**, $400,000 penalty - Care New England Health System (CNE) a healthcare system that acts as a BA to its hospitals and providers
- Breach in 2012: lost or stolen unencrypted backup tapes at one of the system hospitals, led to later investigation
- During investigation, hospital provided its BAA with the system dated 2005, but not updated for 2010 or 2013 changes until 2014

Security Risk Assessment Must Be Done, And *Re-Done* If Things Change

- **October 2016**, $2.14m penalty – St. Joseph Health, a large system operating hospitals, SNFs, and other services in Texas, New Mexico, and California
- In 2011 and 2012 the entity had systems that were not secure and technically incorrectly configured such that internet user could access PHI without credentials
- Failure to conduct security risk assessment; failure to review and evaluate after cyber-system upgrade

Hybrid Entity Needs to Be Careful

- **November 2016**, $650,000 penalty – University of Massachusetts at Amherst
- Failure to separate hybrid entity components; failure to conduct security risk assessment; failure to follow Security Rule; failure to detect malware on system that exposed 1600+ patients records to unauthorized access
- OCR notes that the relatively low fine was because the University was in fiscal crisis (or it would have been higher)

©2017 Cox & Osowiecki, LLC

Breach Rule And Timely Notification Critical (Plus Paper Counts)

- **January 2017**, $475,000 – Presence Health Network (multi-state SNF and home health company, OCR Midwest Region)
- 800 paper files went missing in October 2013
- Breach not reported to individuals for 104 days
- OCR investigation found pattern of failing to timely notify individuals (and OCR)
- Resolution Agreement: “Each day on which Presence Health failed to notify [HHS, the media, individuals] indicates a separate violation of the Breach Notification Rule.”

©2017 Cox & Osowiecki, LLC

Implementing Safeguards Critical (Policies Alone Not Enough)

- **January 2017**, $2.2m -- MAPFRE Life Insurance Company of Puerto Rico (MAPFRE)
- Unencrypted USB drive stolen 2011 (2,209 individuals)
- Representations made in breach report were inconsistent with findings on investigation
- MAPFRE failed to encrypt or update security controls **until 2014**; failed to perform or update security risk assessment

©2017 Cox & Osowiecki, LLC

Don’t Ignore HHS Letter, Redux (Oh, and Security Implementation Is Required)

- **February 2017**, $3.2m -- Children’s Medical Center of Dallas (CMCD)
- Never responded to the HHS investigation letter – so full CMP assessed
- CMCD in 2010 reported a 2009 loss of unencrypted Blackberry device
- During investigation, OCR found that CMCD had two security risk assessments performed between 2007 and 2008, with gap analysis showing failure to encrypt portable devices – still failed to encrypt

©2017 Cox & Osowiecki, LLC

Poor Audit Controls; Poor Termination Process For Users Creates Huge Security Gap

- **February 16, 2017**, $5.5m penalty - Memorial Healthcare System (MHS), healthcare system in South Florida. $5.5 = $1.5m for each year the issue was not resolved
- MHS reported that two former employees 2011-2012, accessed 115,143 individuals' files (and committed fraud and identity theft activities)
- During investigating that, MHS also found 12 individuals who were still logging in with old credentials and sharing PHI to affiliated physician office staff
- Also log in credentials of former practice employee used to access 80,000 files

©2017 Cox & Osowiecki, LLC

Security Risk Assessment Is Critical

- **April 2017**, $400,000 penalty. Metro Community Provider Network, an FQHC in Colorado.
- Hacker obtained 3,200 patients' files through unauthorized access to an employee account ("phishing" attack)
- No risk assessment prior to event
- Slow to react post event (3 weeks passed before risk assessment was done)
- Risk assessment was insufficient to meet the Security Rule (not robust enough)

©2017 Cox & Osowiecki, LLC

You Really Need To Have BAAs

- **April 2017**, $31,000, Center for Children's Digestive Health, seven clinics in Illinois
- Center didn't have a BAA with its **paper records storage company**
- BAA was under investigation for something else
- During unrelated investigation, OCR asked for all BAAs -- neither Center nor BA could produce one

©2017 Cox & Osowiecki, LLC

Digital Health Companies Should Know About the Security Rule

- **April 2017**, $2.5 million, CardioNet, a health technology vendor that provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias
- Stolen, unencrypted laptop…*but wait there's more*
  - Security Policies were never adopted
  - CardioNet was only able to produce policies still in "draft" form
- "Mobile devices in the health care sector remain particularly vulnerable to theft and loss….This disregard for security can result in a serious breach, which affects each individual whose information is left unprotected."

©2017 Cox & Osowiecki, LLC

Disclosure Permission Is Not Transferrable

- **May 2017**, $2.4 million, Memorial Hermann Health, 16 hospital system in Houston area (Texas)
- Patient fraudulently presented as someone else. Police were called (fraud, identity theft). All fine and HIPAA compliant until that point
- Hospital issued press release about the incident and **included** the person's name. Privacy rule violation.
- OCR: "This case reminds us that organizations can readily cooperate with law enforcement without violating HIPAA, but that they must nevertheless continue to protect patient privacy when making statements to the public and elsewhere."

©2017 Cox & Osowiecki, LLC

Sending to the Wrong Place Is Bad – Sending Sensitive PHI Is Worse

- **May 2017**, $387,200, St. Luke's-Roosevelt Hospital Center Inc., a hospital in a seven hospital system, operating a service for patient's living with HIV
- Hospital faxed patient's sensitive information (HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse) to his employer rather than sending it to the requested personal post office box
- Provider also had a related breach of sensitive information nine months prior but had not addressed the vulnerabilities

©2017 Cox & Osowiecki, LLC

Resolutions Since May 2017….

None.

Will the pace continue?

©2017 Cox & Osowiecki, LLC

OCR Link

- OCR keeps running list of Resolution Agreements on its website:

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/

©2017 Cox & Osowiecki, LLC

Questions

©2017 Cox & Osowiecki, LLC