IMPROVING INTEROPERABLE SYSTEMS WHILST PROTECTING THE PATIENT

SETH CUTLER - CSO, ALLSCRIPTS

JULY 17TH, 2018

AGENDA

- Introduction
- Interoperability Challenges
- Keeping the Data Secure
- Futures
- What Should We Be Doing?
- Q&A

INTRODUCTION – SETH CUTLER

- VP & Chief Security Officer (CSO) at Allscripts (NASDAQ: MDRX, $3B, 10K Employees)
- Software Development for ~30 years
- Board of Directors NCHICA
- Member of ISC2 (HCISPP), ISSA, FBI-InfraGard, ISACA, NH-ISAC, IAPP, Cyberhealth WG
- Speaker at ACE, HIMSS, Privacy/Security Conferences

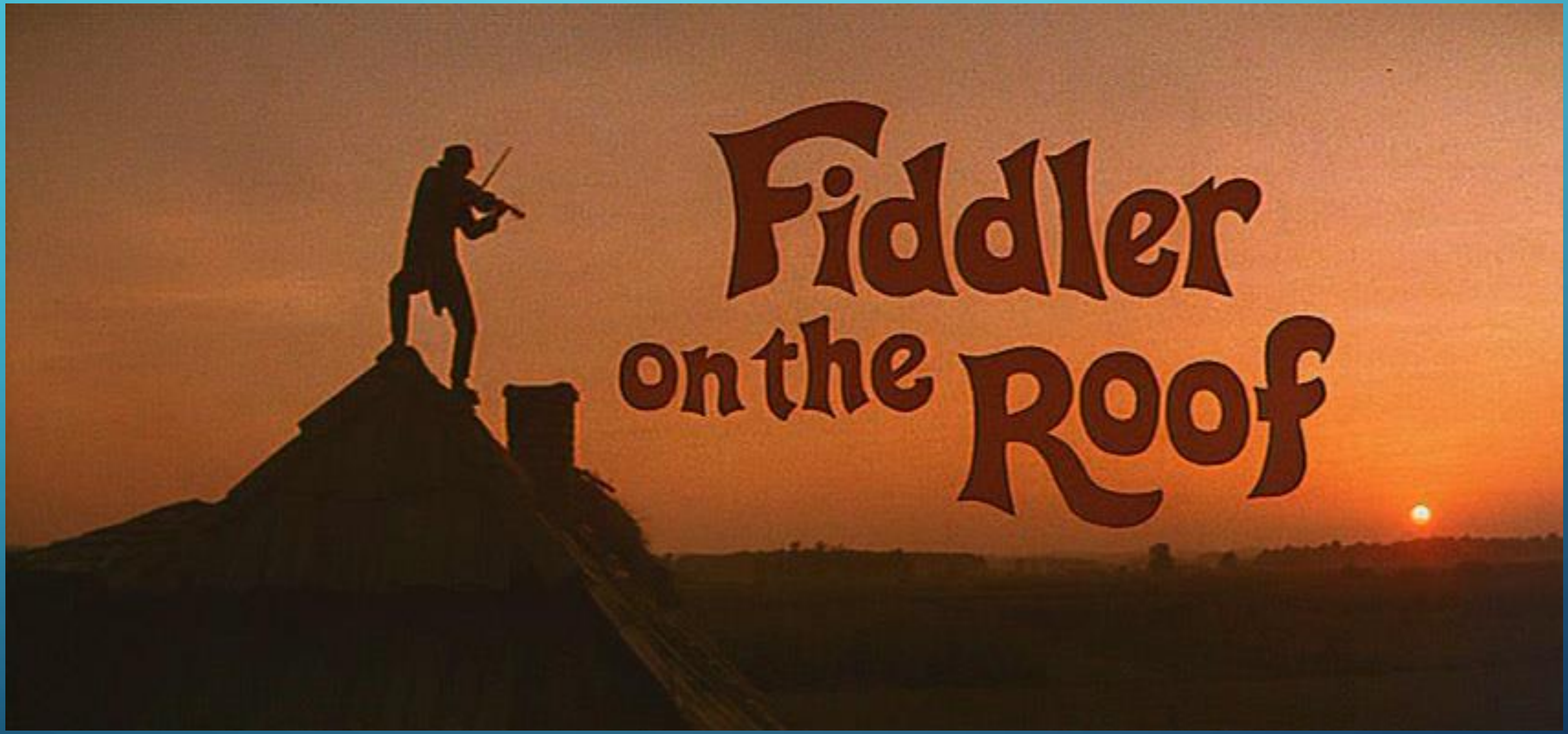
DEFINITIONS OF INTEROPERABILITY

- HIMSS View:
  - **Foundational** – Enables one information system to exchange data with another information system. The system receiving this information does not need to have to interpret the data. Instantly available for use.
  - **Structural** - Defines the format of the data exchange. Standards that govern the format of messages being sent from one system to another, so that the operational or clinical purpose of the information is evident and passes through without alteration.
  - **Semantic Interoperability -** Highest level of connection. Two or more different systems or parts of systems can exchange and use information readily. Structure of the exchange of data and how the data itself is codified lets medical providers share patient data even when using completely different EHR software solutions from different vendors.

ONC VIEW

- Section 4003 of the 21st Century Cures Act, the term 'interoperability,' with respect to health information technology, means such health information technology that— "(A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
- "(B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
- "(C) does not constitute information blocking as defined in section 3022(a)."

TEVYE PROBLEM…



Need to balance a lot… (Will need to break Tradition!)

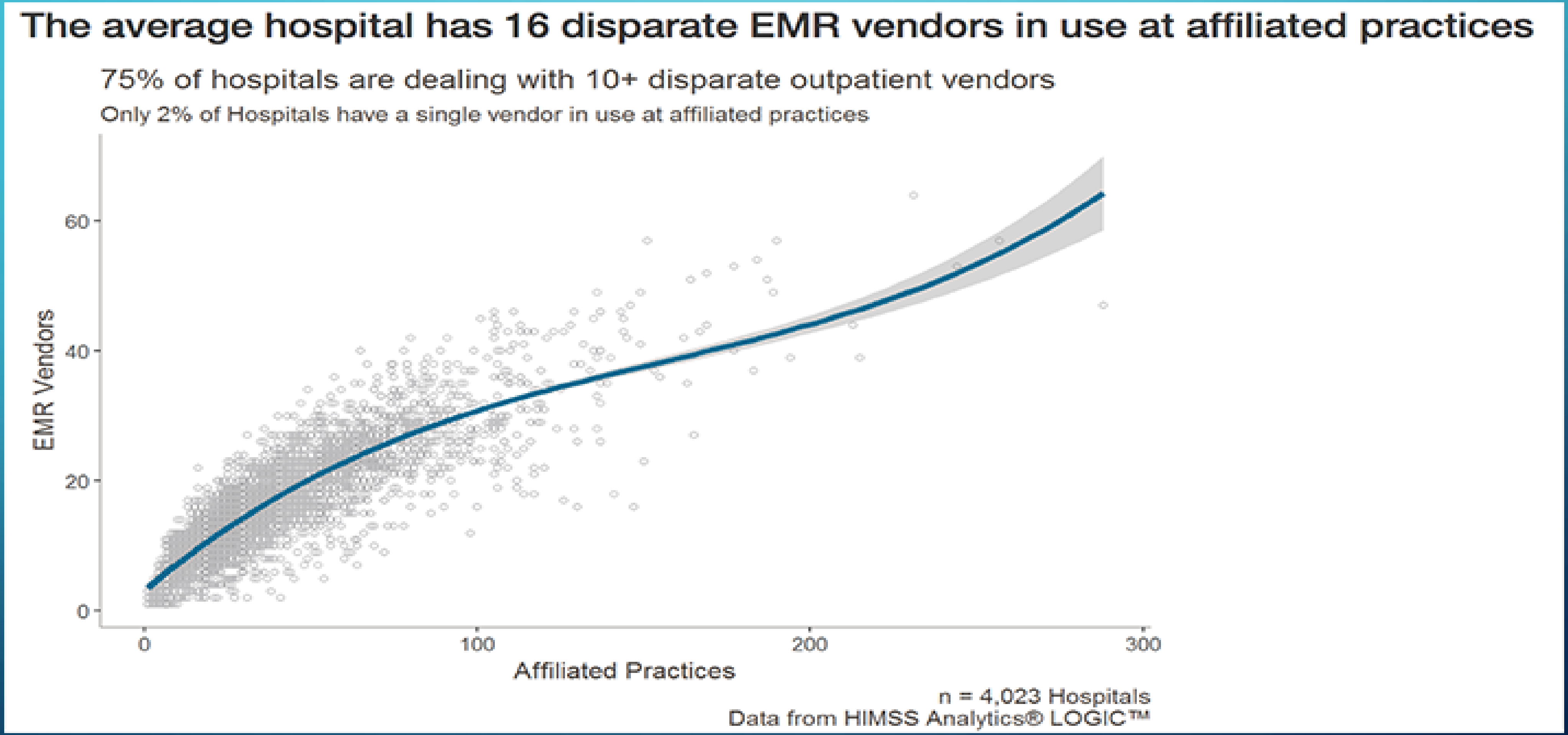
INTEROPERABILITY CHALLENGES

- Ever-growing eco-system
  - Cloud, HIEs, HISPs, IoT, endless devices, mobile, M&A, wearable/PGHD, precision medicine
  - “No vendor left behind…”
  - Multiple EHR’s within a health system
- Outdated eco-system
  - Continued reliance on Fax/Paper/Courier
  - Security standards not current in the eco-system (IoT, MRI…)
- Many standards, networks, and platforms
  - CommonWell, CareQuality, HIEs, NATE, OAuth, HL7/CCDA/FHIR…
  - Tough to stay current

INTEROPERABILITY CHALLENGES – CONT'D

- CMS & ONC focus on interoperability
  - 21st Century Cures/TEFCA
  - ONC 10 Year Vision
- Ever-changing workflows , definitions of interop, tons of use cases
- Tough to harmonize data
- Federal, jurisdictional and privacy concerns
  - Appropriate Use, Consent, Minors, Behavioral, Reproductive, VIP, etc
  - General privacy concerns – want to be compliant
- Patients & Providers want the full data and provenance
  - Follow the patient **AND** secure

HIMSS ANALYTICS



The average hospital has 16 disparate EMR vendors in use at affiliated practices

75% of hospitals are dealing with 10+ disparate outpatient vendors

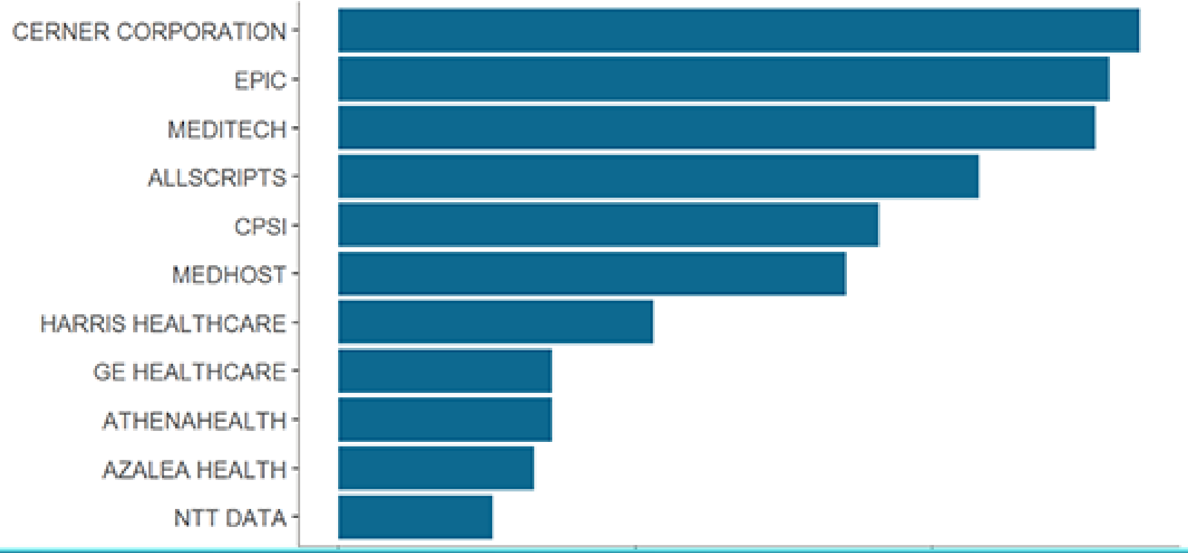
Only 2% of Hospitals have a single vendor in use at affiliated practices

n = 4,023 Hospitals
Data from HIMSS Analytics® LOGIC™

MORE DATA…

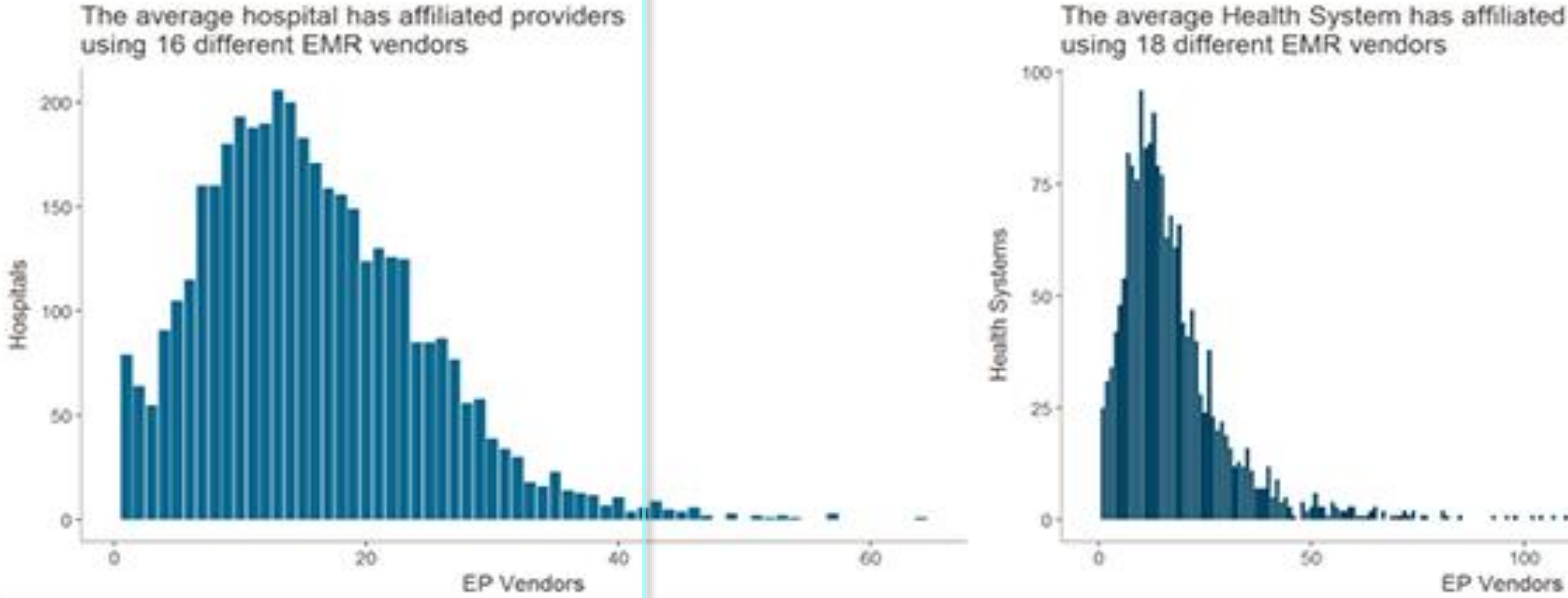
Acute EMR vendors average 82 disparate EMR vendors used by providers affiliated with their in-patient clients

That's a different vendor for every 106 affiliated providers



HIMSS Analytics Data…

Disparate Outpatient EMRs


The average hospital has affiliated providers using 16 different EMR vendors

The average Health System has affiliated using 18 different EMR vendors

WHAT DOES THIS ALL MEAN?

OPPORTUNITY….

Ever-growing attack surface for the bad guys

SOLVING INTEROPERABILITY WITH SECURITY/PRIVACY IN MIND

- System of Systems Engineering (SoSE) → Airplane Analogy
- Open/Secure APIs
  - CommonWell/CareQuality (Identity Proofing, TLS, FHIR, SAML, REST…)
  - FHIR – DirectTrust, DevDays, Devices of FHIR (DoF), Connect-a-thon's
- Token usage → OAuth
- MyHealthEData (CMS - 3/18)
  - Initiative to put Patient at the Center
  - "Secure patient access"
- TEFCA - ONC's Trusted Exchange Framework and Common Agreement (1/18)

SECURING THE DATA

- CORNERSTONE - Confidentiality, Integrity, Availability (CIA) Triad
    - Identity, Authorization, Authentication, Login, Privacy, Consent
    - Patient Safety concerns?
- Secure the pipe – data in transit
- Secure the record – who has access? are they authenticated?
- Make it available and in the correct context

INTEROPERABILITY – WHERE ARE HEADED?

- Will there only be one? NOT LIKELY
- Google, Amazon, Apple
  - Cloud-Based
  - AI-Assisted
- BlockChain
- Other innovator's NOT in the Health Space (“Consumer Health Apps…”)

BLOCKCHAIN

- Not just Bitcoin…
- Use cases growing in healthcare
- Data organized so EHR transactions verified and recorded through consensus
- Every action is verified against a “Ledger”
- May help with consent, provenance, security, patient safety
- ONC continuing to explore the use

WHAT DO WE NEED TO DO?

- Open AND Secure API data exchanges for all (THINK AGNOSTIC)
- Segment the Data (DS4P/CCDA)
- ALL Vendors MUST bring the standard up for security (a weak link…)
    - FDA Guidance, NIST, OWASP
- Comment on ALL standards recommended for interop – CMS/OCR/HHS Guidance
- Continue the push for EHR vendors to operate seamlessly
    - No closed end (ATM Model?)
    - Remember the goal → comprehensive, secure, contextual view of the data
- Keep eye on the International standards (GDPR)

WHAT DO WE NEED TO DO – CONT'D?

- ONC Roadmap
  - Strong & effective data security safeguards
  - Stable, trusted, secure, widely available network capability that supports technology developer-neutral protocols and a wide variety of core services" for an interoperable and learning health system
- MFA where appropriate
- Data encryption standards current
- Training and awareness
- Technical, Physical, Administrative safeguards current?
- Drill, test, assume breach – are you prepared?

THANK YOU – Q&A?

BACKUP

GLOSSARY

- Trusted Exchange Framework and Common Agreement (TEFCA) - designed to support nationwide interoperability by outlining a common set of principles, as well as minimum terms and conditions for trusted data exchange. January 2018 21st Century Cures.
- CommonWell Health Alliance – non profit trade association dedicated to achieving cross-vendor interoperability that assures provider access to health data regardless of where care occurs. Patient linking and matching, CCDA.
- CareQuality - Based on Interoperability Framework (non profit Sequoia Project). Trusted exchange, query based document exchange. Covers legal and technical.
- DirectTrust – Collaborative non-profit. Created a trust framework.

GLOSSARY

- eHealth Exchange – Sequoia Project Interoperability Initiative (NwHIN)
- FHIR -Fast Healthcare Interoperability Resources. Latest standard developed by the HL7 organization.
- NATE – National Association of Trusted Exchange. not-for-profit membership association focused on enabling trusted exchange among organizations and individuals with differing regulatory environments and exchange preferences
- OAuth - Open Authorization is an open standard for token-based authentication and authorization on the Internet. Allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password
- Argonaut Project – Private sector initiative to rapidly develop a first-generation FHIR-based API and Core Data Services (HL7 FHIR Project)