Strategies to effectively monitor researchers' access to the EMR

Daniel Fabbri
Founder and CEO, Maize Analytics
Assistant Professor, Biomedical Informatics, Vanderbilt University

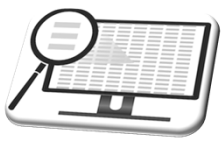
Agenda

- Background on EMR monitoring and researcher PHI access
- Methods to monitor researcher access within health systems
- Tactics for facilitating a culture of research compliance

2

Standard PHI Monitoring Programs

- Monitor employees' accesses to the EMR:
  - Nurses
  - Doctors
  - Clinical Staff
- But what about researchers?



3

Researchers and PHI

- Medical centers often support clinical research
- Research activities involve:
  - Cohort creation
  - Chart review
  - Population health analytics

- Thus, researchers require access to PHI to complete their job

4

Examples of my research projects

Pediatrics
July 2015
From the American Academy of Pediatrics
Article

Predicting Discharge Dates From the NICU Using Progress Note Data

Michael W. Temple, Christoph U. Lehmann, Daniel Fabbri

Journal of Biomedical Informatics
Volume 74, October 2017, Pages 59-70

Classifying patient portal messages using Convolutional Neural Networks

Lina Sulieman [a], David Gilmore [b], Christi French [b], Robert M. Cronin [a, c, e], Gretchen Purcell Jackson [a, d, e], Matthew Russell [b], Daniel Fabbri [a, f]

5

How do researchers access PHI?

- Through the EMR (chart review)
- Through the backend data warehouse (SQL)
- Through ad-hoc tools in the institution

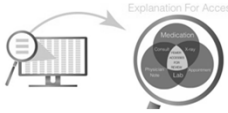
6

Researchers can be a threat to patient data

- Similar to standard clinical staff, researchers are susceptible to:
  - Curiosity (snooping)
  - Phishing (stolen credentials)
  - General inappropriate access
- Therefore, robust monitoring programs should include researchers

Traditional PHI Monitoring Methods

- **Statistical Anomaly Detection:** Does the access look 'normal'?
- **High-Risk Flags:** Same last name, co-worker, VIP, etc.
- **Explanation-Based Auditing**: Determine TPO reason for access



8

Challenges of monitoring researchers' access

- Researchers are <u>not</u> part of treatment or operations
- Researchers' accesses often appear as 'outliers' or 'random' accesses
- Flagging approaches have high-false positive rates

9

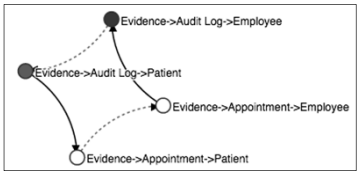
Observations

- Most accesses by researchers are appropriate
- Researchers access PHI after attaining IRB approval
- Researchers focus on specific cohorts of patients

10

Explanation-Based Auditing

- Learn why each access occurs



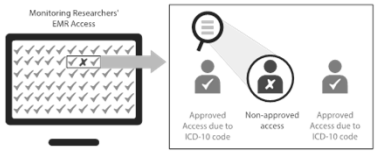
Find connections between patient and employee access the patient's record

Published in VLDB 2011 and JAMIA 2012

11

Can we identify the reason for a researcher's access?

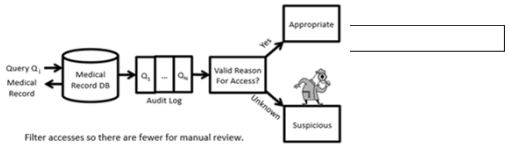
- Leverage information about patient cohorts (ICD codes)



12

Filter out appropriate research accesses

- Identify accesses to approved research cohort
- Analyze accesses that are not filtered (unexplained accesses)



Filter accesses so there are fewer for manual review.

13

Data exchange between IRB and Compliance

- Modify IRB submission process to collect structured data
  - ICD codes
  - CPT codes
  - Age
- Send approved IRB meta-data to compliance for research monitoring

14

Modern EMR Research Managers

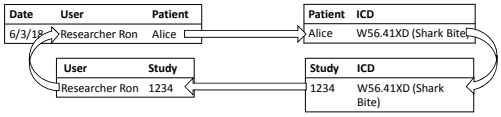
- Popular EMRs have research manager systems
- The managers tracks:
  - Researchers' assignment to studies
  - Patients' assignment to studies
- These assignments can be pulled from backend reporting systems

15

Develop research auditing policy

- Filter accesses if:

*"The researcher is part of study **X**,*
*Study **X** is approved to analyze patients with ICD diagnosis **Y**,*
*The researcher accessed patient **P** who has diagnosis **Y**."*



16

Research Access Audits

- Review accesses that have no reason for access:
  - Outside of defined cohort
  - No supporting ICD code or study list
- Can require researcher 'interviews'
- Adjust cohort descriptor, as needed

17

How do researchers access PHI?

- Through the EMR ✓
- **Through the backend data warehouse** ?
- Through ad-hoc tools in the institution ?

18

Back-end Data Warehouse

- Many researchers use SQL queries on EMR databases
  - Still considered "access" to ePHI
  - Privacy and Security rules for monitoring apply
- SQL logs do not map to patients
- SQL queries are decipherable only to technical users

19

Many different types of SQL access patterns

- **Broad**: SELECT * FROM patients
- **Specific**: SELECT * FROM patients WHERE name = 'Taylor Swift'
- **Automated / Nightly**: SELECT * FROM patients WHERE time = YESTERDAY()

20

SQL Monitoring

- Automate monitoring of researchers' access to SQL database
- Identify attributes/context in queries:
  - Which tables were accessed?
  - Which patient records were touched?
  - Were the patients accessed part of the defined cohort?

21

SQL access audits

- Audits done by a multi-disciplinary team: Info. Security and Compliance
- Need to translate technical access patterns to compliance access policy
- Adjust SQL database access rights, as needed

22

Facilitating culture of compliance

- Develop strategy for research access monitoring roll-out
- Create an education plan for internal awareness
- Actively monitor research access

IRB Submission Process

- Modify current IRB submission forms
  - Require structure fields (ICDs) to define patient cohorts
  - Explicitly list patients in cohorts, if possible
  - Require researchers specify method of data access (EMR, SQL, etc.)
- Meet with research department heads
  - Hear concerns
  - Attain buy-in
  - Take care to limit additional PI effort

24

EMR workflow for clinical researchers

- Some clinical staff wear `two hats'
- Adjust EMR login process – select 'Researcher' login department
- This explicit demarcation allows auditors to focus on researcher access

25

Education Plan

- Inform researches of monitoring ahead of time
  - Collateral
  - Policy attestation
  - Administrative staff support
- Potential non-punitive "grace-period"

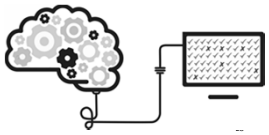
Launch of program

- Present intention of monitoring access during IRB submission process
  - Require PI signatures on your "Access Policy Statement"
  - Include all PHI accessing users on IRB application
- Focus on education training for current and new researchers

27

Continued monitoring efforts

- Follow-through with active monitoring
  - Set procedure to meet "Reasonable Effort"
  - It only takes one user to be found; word spreads quickly
- Continue with proactive education
  - New students/researches



Summary

- Researchers are not exempt from Privacy and Security Rules
- IRB submission process: Gather structured data
- Monitoring Tools for EMR access and SQL access
- Implement Tactfully: Awareness and continuing education

29

Questions?

Daniel Fabbri
Founder and CEO, Maize Analytics
Assistant Professor, Biomedical Informatics, Vanderbilt University
dfabbri@maizeanalytics.com
615-997-0101 ext. 700

30