The Dark Side of the Cloud

How a lack of EMR security controls helped amplify the Opioid crisis and what we can do about it

Indiana University Health

Why are we here?

- The Opioid crisis has caused mass addiction of prescription painkillers
- Tens of thousands have died from this
- Families have been broken apart
- Children have been born addicted
- It has stretched the social support network we have to its breaking point

Why am I talking about this at Black Hat?

- A major root cause of this crisis was due to underhanded manipulation of an Electronic Medical Records (EMR) system used to assist physicians in prescribing medications
- An EMR company settled for $145 million with the US Justice Department for allowing the Marketing department of an opioid manufacturer to manipulate the system to recommend their products
  - **People died and became addicted because of this**
- Subversive manipulation of electronic systems is a security issue
  - And one that we have not addressed for smaller organizations

Who was the EMR company?

- Practice Fusion – now a division of Allscripts
- They started as an independent company that provided an ad-supported free EMR
- The business model was controversial because of perceived violations of the Stark Act and the Anti-Kickback Statutes due to ads
- In 2015, they missed financial goals and their Founder and CEO, Ryan Howard, stepped down
- In 2018, they were acquired by Allscripts for $100M under a cloud of suspicion of investigations (1/15 expected market value)

Who were their customers?

- Smaller practices that could not afford the large EMR systems or to even lease EMRs from large providers such as UPMC or Mercy
- Practice Fusion had approximately 100,000 practices as customers in 2018

What are some numbers? Why is this important?

- According to the American Medical Association's Policy Research Perspectives Report on ownership benchmarks, 56.5% of patient care physicians worked in practices of 10 or fewer physicians in 2018 (n=3339) [1]
- From the same source, 54% of physicians owned their own practice in 2018 (n=3500) [1]
- From the AMA's PRP on physician compensation (2016 data), 64.2% of physician practice owners based their salary on personal productivity (n=2900) [2]
- Source: https://www.ama-assn.org/system/files/2019-07/prp-fewer-owners-benchmark-survey-2018.pdf
- Source: https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/member/health-policy/prp-how-physicians-paid.pdf

What does this mean?

- This means that physicians work to pay the bills like the rest of us, and their income is mainly based on how many patients they see and how much they bill
- The margins to hire employees when the owners work that much is not good enough to have the specialists you are going to have in large health systems
- In addition, according to the American Hospital Association's 2018 chartbook, 26.4% of hospitals have negative total margins and 30.6% have negative operating margins [3]
- Yet we have the same EMR requirements across the board
- Source: https://www.aha.org/system/files/2018-05/2018-AHA-Chartbook_0.pdf

What is an Electronic Medical Record?

- According to HealthIT.gov:
  - **Electronic medical records (EMRs)** are a digital version of the paper charts in the clinician's office. An EMR contains the medical and treatment history of the patients in one practice. EMRs have advantages over paper records. For example, EMRs allow clinicians to:
    - Track data over time
    - Easily identify which patients are due for preventive screenings or checkups
    - Check how their patients are doing on certain parameters—such as blood pressure readings or vaccinations
    - Monitor and improve overall quality of care within the practice
- They also now interface with other health systems, payors, and business associates

How do they work?

- They have many interfaces:
  - Remote Desktop/VDI/Citrix
  - Web
  - Mobile Device App
  - Desktop App
  - Data interfaces for med devices, billing systems, etc.
- They normally authenticate from a directory service
- They also often have remote access from off-site
  - A major demand for this has been for physicians to complete charts after hours

Security Holes in systems for smaller practices

- EMRs need to be certified to be eligible for federal reimbursement dollars and for use to store patient records
  - Done by the Certification Commission on Health Information Technology (https://www.cchit.org/about/)
- However, certification is only one part
- Organizations have to complete annual risk assessments and complete risk management plans
- They also have to follow up on security findings
- Failure to comply can result in fines from the Office For Civil Rights of the Department of Health and Human Services

What does every OCR penalty have in common?

- We went through every HHS press release on HIPAA settlements issued since 2015 from the HHS web site: https://www.hhs.gov/ocr/newsroom/index.html
- We identified the following five key factors for an OCR penalty:
  - No Risk Assessment Completed
  - No Risk Management Plan Completed
  - No Follow up on Risk Assessment
  - Not Properly Reporting Breaches Within 60 Days
  - Underreporting Breaches
- Many of these organizations were multi-billion-dollar systems
- If they're not doing these, your average small practice isn't either

If they're not doing those, they aren't doing these either

- Reviewing changes to the EMR system
- Reviewing changes to clinical decision support alerts
- Reviewing access levels
- Providing relevant training that doesn't check a box

What are other complicating factors?

- Pretexting Attacks
  - Due to information being made available on medical staff on the Internet there has been a sharp uptick in these calls to medical staffs
    - Criminals claiming to be government regulatory agencies or professional associations asking to “update their information” using spoofed caller ID or emails
    - Not difficult to get personal info using this method and then use that to call a Help Desk and get a hold of someone’s username and password
    - System access!

Three step method – yes there is a Phase 2

- Phase 1: Get National Practice Identifiers and Public Information from Internet
- Phase 2: Call Practices and get personal info using spoofed Caller IDs
- Phase 3: Profit! (especially with no two-factor authentication)

What are other complicating factors?

- Lack of two-factor authentication for system access
  - While prescription of opioids does require two-factor authentication, base system access often does not
    - This means you can make changes to processes requiring 2FA without actually needing 2FA to do so!
  - This includes administrative access to EMR systems
  - This is not a failing of any EMR system in itself – a failing in how to protect them!

Isn't this just theoretical?

- No
- Practice Fusion demonstrated exactly how to do it
- They revealed flaws in how we secure EMRs that we need to fix

Who were they?

- They were a company started in 2005 by Ryan Howard (definitely not the ex-Phillies MVP)
- They provided an ad-supported free Electronic Medical Records system to doctors available in the cloud
  - This meant less IT investment
  - Key when almost 2/3 of your salary is based on seeing patients
  - You have to see a lot to afford IT and keep the lights on
  - You're not spending money on compliance if you cannot afford a high-end EMR
- Most of their revenue, according to the Washington Post, came from ads

That's a problem, isn't it?

- According to the Anti-Kickback Statute [42 U.S §1320a-7b(b)], yeah

- The Anti-Kickback Statute is a criminal law that applies broadly and prohibits the knowing and willful payment of remuneration to induce or reward patient referrals or the generation of business involving any item or service payable by the Federal health care programs. Keep in mind that the remuneration can be anything of value such as cash, below market value rent, or relief of financial obligations

- **Translation: Ads in a product used to receive money from federal incentive programs is going to eventually land you in serious trouble**

Clinical Decision Support Alerts

- According to the US DOJ settlement, they had another line of business
- They marketed themselves to drug manufacturers as willing to customize clinical decision support alerts
- Pharma Co. X, according to this settlement, paid $1M to add custom clinical decision support alerts to their EMR
  - Pharma Co. X is still under an active criminal investigation
- These alerts, written by unqualified personnel, recommended extended release opioids to doctors **230 million times** between July 2016 and the spring of 2019
- Doctors who received these alerts prescribed them at a higher rate than those that did not

Deception = Death

- Subversion of the computer system used to provide false information caused the false prescription of extremely addictive drugs in the middle of a crisis
  - **People died and became drug addicts because of a marketing department**
- It illustrated security holes that affects smaller providers

How can we address this?

- We're going to show you how we can address this using four methods:
  - More clarification of the Stark Act Safe Harbors to allow larger providers to provide cybersecurity services to smaller ones
  - Having smaller providers leverage the resources of larger ones to provide Clinical Decision Support Services to their EMR instances
  - Including Privacy and Diversion Monitoring Services as part of the bundles of services sold
  - Increasing security in the EMR itself to require two-factor authentication and increased logging around creating alerts or making configuration changes

Stark Act Safe Harbor Wording

- 42CFR §1001.952(c)(5) requires fair market remuneration for equipment rental and is not based on the volume or value of referrals
- 42CFR §1001.952(d)(5) requires fair market value remuneration for management services
- 42CFR §1001.952(y)(11) requires that practices pay 15 percent of the cost of services upfront

What is being proposed

- In October 2019, the Department of Health and Human Services proposed an amendment to 42CFR §1001.952 to allow for donation of cybersecurity products and services [4]
  - However this did not include patching, maintenance, and hardware
- In January 2020, the Health Sector Coordinating Council proposed further amendments, including: [5]
  - Patching and maintenance
  - Hardware
  - Liability Protection for Donors

[4] https://healthitsecurity.com/news/hscc-tells-hhs-include-patching-in-stark-law-cybersecurity-donations

[5] https://healthsectorcouncil.org/hph-scc-cybersecurity-working-group-comments-on-oig-and-cms-companion-proposed-rules-rfi/

What we propose

- We propose further amendments to include:
  - Diversion Monitoring Software – Allow for donation of services to include drug diversion monitoring in practices and alerts of potential issues
  - Privacy Monitoring – Allow practices to monitor/be alerted to potential patient privacy violations by donation of the use of privacy monitoring software
    - Why? Because ID theft from smaller practices happens and can lead to further fraud: https://www.healthcareinfosecurity.com/inside-job-at-clinics-mobile-phone-used-for-fraud-a-14364

Leveraging Larger Providers Whenever Possible

- Leverage partnerships or reseller agreements with larger health systems or service organizations to use their EMR systems under paid contract
  - Use their expertise (and staffing) to help create/monitor CDS alerts
  - Leverage their order sets and alerts to reduce opioid prescriptions
  - Have larger systems include managed Privacy and Diversion monitoring in their packages

Privacy and Diversion Monitoring Services

- The most recent survey we could find was from the Ponemon Institute in 2016, which indicated that 56% of providers had sufficient privacy protection [6]
- However, 2% of respondents to that survey, with n=90, were from organizations of less than 100 people
  - Benchmark surveys in healthcare normally are biased toward larger institutions
  - This means we have no data demonstrating the real situation
  - We need to make sure these services are offered
- Diversion monitoring is new, however there is a demonstrated need
- [6]https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

Privacy and Diversion Monitoring

- We can't talk about security without privacy and diversion
- You're protecting against malware, worms, and ransomware
- However, you're not protecting against ID theft, diversion, and their cascading effects
- And definitely not curious team members looking at medical records and using that info for personal gain

Security in the EMR Itself

- EMR vendors have done an incredible job with security improvement
  - I have worked with several in this area
- There is two-factor authentication for prescribing opioids
  - And numerous companies selling great solutions for it
- However, there is potential room for improvement

Security in the EMR Itself

- These are four areas we can improve:
  - Requiring two-factor authentication to make administrative or configuration changes, not just prescribing
  - Limiting access to who can make changes in the EMR
    - As part of cybersecurity services provided, this needs to be in there
  - Making it easier to provide configuration change reports of what changes were made
  - Working with providers to ensure that access to their systems is fully secured and using 2FA

What are our takeaways?

- Smaller practices are more susceptible to electronic subversion of their critical systems because of lack of resources to examine how they operate
- Partnerships with larger health systems are key to addressing resource needs with Electronic Health Records, not just in cybersecurity
- Waiving the Stark Act provisions for cybersecurity and adding guidance for privacy and diversion monitoring will greatly help smaller providers address what we've discussed, along with security issues
- We need to improve security in several areas with EMRs

Thank you!

- Follow me on Twitter @mitchparkerciso