Cybersecurity, Blockchains and Healthcare

Emily Vaughn, Blockchain Product Director, Change Healthcare
Exponential growth in healthcare transactional data

2013: 153 exabytes
2020: 2,314 exabytes
150% CAGR

Source: International Data Corporation
Healthcare data exchange faces many challenges

- Lack of interoperability
- Target of many cyber-attacks
- Lag in data accessibility
- High administrative spend
Blockchain technology is part of a transformation that’s already underway in healthcare.

We all want a future where information is:

• Immediately available
• Identical everywhere it is stored
• Has a complete history
• Is immutable
• And is user-centric – “controlled” by the contributor
Blockchains are like an accounting system for an entire industry.

They keep track of information between people and companies.
Today - Each party has a different version of events for a claim.

Patient responsibility is increasing, but patients don’t understand their bills. Patients don’t understand their options for healthcare services.

Providers lose $20 - $30 billion dollars annually due to errors in the claims process. This loss contributes to the rising cost of healthcare.

Estimates for the cost of fraud, waste and abuse in healthcare range from $80 - $250 billion dollars annually. Payers increase deductibles and patient share.
With a blockchain - Each party has a shared version of events.
The value of blockchain....applied to healthcare

- Disintermediation & trustless exchange
- Empowered users
- High quality data
- Durability, reliability, and longevity
- Process integrity
- Transparency and immutability
- Ecosystem simplification
- Faster transactions
- Lower transaction costs

Blockchains are identical event logs that connect applications and users directly.

They are so secure and transparent, that applications use it to track digital units of value between them (tokens, data, code, etc.)
What is a blockchain?

**Information Storage** - the event log

**Consensus Model** - how events get added to the log

Associated with blockchains
- Public Blockchains
- Permissioned Blockchains
- Private Blockchains
- Smart Contracts

Not a feature
- Interoperability
- Encryption of data
- Participant lists
- Speed (real-time)
What is a blockchain? – Information Storage

It’s a list of transactions, grouped into Blocks, and locked immutably together forever.
What is a blockchain? – Consensus Model

50% + 1: Majority rules

Trust Issues...
• Proof of Work (Bitcoin): compete to add by solving a puzzle
• Proof of Stake: more coins you own, better your odds
• Proof of Activity: combines Work + Stake
• Proof of Burn: Irretrievable “pay to earn”
• Proof of Capacity: The more storage, the better the odds
• Proof of Elapsed Time: Waiting to win (Intel)
Blockchains ≠ cybersecurity

Blockchains are not a cybersecurity solution. Their features have cybersecurity implications; they can pose benefits or challenges depending on configuration.
Blockchain transaction data is immutable.

If the business process actually ‘rewrites’ history, and appended structures are not more valuable, blockchains are not the right choice.

If the business process does not value historical or referenceable data, blockchains are not the right choice.

If the business process stacks updates on top of the original record to show the history of modifications, blockchains are a candidate. Most processes are like this one.

Blockchains track unique data assets - “nouns.” It records the history of verbs that occur to those nouns.
The speed or latency of a blockchain depends on a variety of design choices.

Business processes that are sensitive to time should establish strong success criteria when considering blockchain networks.

Speed and latency is affected by:

- **Blockchain Protocols:** (Hyperledger Fabric, Iroha, Sawtooth Lake; Ethereum; etc.)
- **Consensus Models** (PoW, PoET, etc.)
- **Block size** (2x)
- **Block management** (Segregated Witness: Segwit, Segwit2x)
Reaching consensus on a blockchain costs processing power. What minimum factors should be agreed to for the network to operate efficiently?

How much energy/power/compute will be required to balance the trust amongst the participants?

The largest trust difference is the driver.

Bitcoin assumes zero trust.

A permissioned Blockchain balances its trust with the process of receiving permission to participate.

This means that consensus rarely focuses on the merit of the users or context of a transaction. Consensus is about meeting technical requirements.
Considering risk in designing blockchain applications

Consider the liability and risks of:

• Submitting a block containing an inaccurate transaction.
• Accepting a transaction from a bad actor to include in a block.
• Unintentionally submitting a bad transaction.
• Providing information to a Blockchain as an oracle that is later found to be invalid (intentionally or unintentionally).
• Calculating a block that contains a banned transaction (financial) between two parties.
• Eventual regulation that varies by (overlapping and/or nested) jurisdictions
Blockchain technology in healthcare is in its early days.

Blockchain technology for data exchange is widely available and innovating.

Blockchains are not a cybersecurity solution, but should be considered in future cybersecurity solutions.
Cybersecurity in Healthcare

A VERY BRIEF OVERVIEW

Douglas Barton, CISSP
Leidos Health CTO and Chief Engineer
Cybersecurity in Healthcare

- Regulatory Requirements
- Cybersecurity Frameworks
- State of the Industry
Regulatory Requirements

- **HIPAA Security Rule**
  - Covered entities/business associates must ensure the confidentiality, integrity, and availability of electronic protected health information (PHI) that they create, receive, maintain, or transmit
  - Specifies organizational (documentation) requirements
  - Specifies 42 administrative, physical and technical security requirements

- **HIPAA Privacy Rule**
  - 45 CFR Part 160 and Part 164, Subparts A & E, “Privacy of Individually Identifiable Health Information”
  - Applicable to same covered entities as the security rule (generally)
  - Addresses permitted and required uses and disclosures of PHI
Regulatory Requirements (cont’d)

- FAR 52.204-21, “Basic Safeguarding of Covered Contractor Information Systems”
  - Addresses protection of federal information on contractor information systems
  - Specifies 15 basic security controls
- DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”
  - Addresses confidentiality of federal information in nonfederal systems
  - References DFARS 252.204-7008, “Compliance with safeguarding covered defense information controls”
  - Requires compliance with NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”
  - Federal Health Information is Controlled Unclassified Information
- FDA Guidance for Industry, “Postmarket Management of Cybersecurity in Medical Devices”
  - Recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices
Cybersecurity Frameworks

- NIST “Framework for Improving Critical Infrastructure Cybersecurity”, February 12, 2014 (AKA: Cybersecurity Framework or CSF)
  - Responds to Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,”
  - Voluntary guidance, based on existing standards, for critical infrastructure organizations to better manage and reduce cybersecurity risk
  - 98 requirements (subcategories) across 5 functions and 22 categories
  - Maps to HIPAA Security Rule and covers ~95 of NIST SP 800-53 security controls
  - Healthcare and Public Health assets are critical infrastructure

- NIST SP 800-171 rev1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016
  - Focused on confidentiality of federal information in nonfederal systems
  - 110 security requirements across 14 control families
  - Covers 88% of NIST CSF requirements
  - May be applicable to pending ONC Trusted Exchange Framework (in draft)
Cybersecurity Frameworks (cont’d)

  - A catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations
  - High impact baselines has 212 security controls and 173 control enhancements
  - The primary framework used for federal information systems

- Other common frameworks
  - HITRUST CSF v9
    - Maintained by the non-profit HITRUST Alliance
  - ISO/IEC 27001, Information Security Management
    - One of a family of ISO security management standards
  - Payment Card Industry (PCI) Data Security Standard (DSS) v3.2
    - Requires by businesses processing credit card payments
Regulations and Implementing Frameworks

- The regulations and frameworks referenced above are not all inclusive.

- The requirements in the regulations are similar, but their applicability varies substantially.

- The implementing frameworks substantially overlap but vary quite considerably in the level of detail expressed.

- Healthcare industry conformance with regulation and adoption of cybersecurity frameworks is evolving.
State of the Industry
Cybersecurity Preparedness
Sixth Annual Benchmark Study on Patient Privacy and Data Security, Poneman Institute, May 2016

- 3% assess vulnerability to a data breach on a monthly basis
- 47% are not confident they can detect loss of patient data
- 89% have had at least one data breach in the last two years
- 37% are not confident controls are in place to detect/respond to a breach
Increasing Pressures on Security of Health Data

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 2013 healthcare data reached</td>
<td><strong>150 Exabytes</strong></td>
</tr>
<tr>
<td>Criminal attacks on healthcare data increased from</td>
<td><strong>33%</strong> to <strong>50%</strong> in 2015</td>
</tr>
<tr>
<td><strong>43%</strong> of organizations lack the information security staff</td>
<td>required to meet their current demands</td>
</tr>
<tr>
<td><strong>71%</strong> of hospitals permit medical staff to BYOD</td>
<td></td>
</tr>
<tr>
<td><strong>19%</strong> have a process in place to correct a patient’s medical record</td>
<td>after a breach</td>
</tr>
<tr>
<td>This is expected to double every subsequent year</td>
<td>A health record is worth <strong>$10</strong> on the black market; value is decreasing, market saturated</td>
</tr>
<tr>
<td>A health record is worth <strong>$10</strong> on the black market; value is decreasing,</td>
<td>market saturated</td>
</tr>
<tr>
<td>All believe staff shortages increase risk of breach</td>
<td>30% say unsecured mobile devices are their greatest security risk</td>
</tr>
<tr>
<td>79% believe there is an increased risk PHI will be exposed</td>
<td>79% believe there is an increased risk PHI will be exposed</td>
</tr>
</tbody>
</table>
Security Threats

Where Do They Come From?
What Are They?
Who Is It?

INTERNAL
- WiFi
- Mobile
- Employees (purposeful, accidental)
- System administrators
- Developer
- Call center
- End user (physician, clinician)
- Maintenance personnel
- Security personnel

EXTERNAL
- Visitors
- Patients
- Organized crime
- State affiliated
- Activists
- Former employees
- Hackers

PARTNERS
- IT service providers
- Subcontractors
- Data transmission services
- Personal health records
- Public health records
- Financial institutions
- Insurance companies
- Cloud providers
## High Cost of Healthcare Data Breaches

2017 Cost of Data Breach Study, Ponemon Institute

<table>
<thead>
<tr>
<th>Industry Classification</th>
<th>Measured in US$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>$380</td>
</tr>
<tr>
<td>Financial</td>
<td>$245</td>
</tr>
<tr>
<td>Services</td>
<td>$223</td>
</tr>
<tr>
<td>Education</td>
<td>$200</td>
</tr>
<tr>
<td>Life Science</td>
<td>$188</td>
</tr>
<tr>
<td>Technology</td>
<td>$165</td>
</tr>
<tr>
<td>Retail</td>
<td>$154</td>
</tr>
<tr>
<td>Communications</td>
<td>$150</td>
</tr>
<tr>
<td>Industrial</td>
<td>$149</td>
</tr>
<tr>
<td>Energy</td>
<td>$137</td>
</tr>
<tr>
<td>Consumer</td>
<td>$132</td>
</tr>
<tr>
<td>Entertainment</td>
<td>$131</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$124</td>
</tr>
<tr>
<td>Transportation</td>
<td>$123</td>
</tr>
<tr>
<td>Media</td>
<td>$119</td>
</tr>
<tr>
<td>Research</td>
<td>$101</td>
</tr>
<tr>
<td>Public Sector</td>
<td>$71</td>
</tr>
</tbody>
</table>
Conclusion

- Majority of respondents to Ponemon survey (69%) agree that healthcare organizations are more vulnerable to data breach than other industries
  - The Cost of Data Breach study supports this conclusion
  - The primary cause is lack of resources (dollars and staff)

- Healthcare organizations are taking steps to enhance their cybersecurity posture
  - 2017 HIMSS Cybersecurity Survey

- Healthcare organizations are not, however, proceeding quickly enough to meet the current and evolving threat
  - Improving the cyber posture of the U.S. healthcare infrastructure is a national imperative
Recommendations

- Healthcare organizations would greatly benefit from assistance to improve their cyber posture
  - Availability of additional information resources specific to healthcare cyber concerns
  - Programs to train cybersecurity staff and motivate cyber professionals to specialize in healthcare
  - Availability of consultative support to assist local cyber staff
  - Funding to accelerate improvement in cyber posture
    - A model is funding to implement EHRs with effectiveness measured against meaningful use criteria along with required certifications
Information Security: A Patient Safety Issue
February 9, 2018

Jennings Aske
Vice President and Chief Information Security Officer
NewYork-Presbyterian
Healthcare Industry – Under Attack

Health care 'disproportionately affected' by data security incidents

Written by Colin Marrs on 2 June 2017 in News

Information Commissioner's Office shows sharp increase in data breach incidents in central government and courts sectors.

ICO releases four years' worth of data on security breaches - Photo credit: Tobias Felber/DPA/Press Association Images
Healthcare Industry “Attack Surface”

- Healthcare is 1/6 of the U.S. GDP
- Nationally there are,
  - 900K physicians, 2.8 million nurses and administrative staff
  - 230K physician practices
  - 5700 hospitals
- What else?
  - skilled nursing facilities, pharmacies, ambulatory surgery centers . . .
- And more to come:
  - 165K mobile healthcare apps, telehealth, “smart” consumer devices . . .
Cyberattack Forces West Virginia Hospital to Scrap Its Computer Systems

By Melanie Evans | Published June 29, 2017 | Features | Dow Jones Newswires

Princeton Community Hospital in rural West Virginia will scrap and replace its entire computer network after being struck by the cyberattack paralyzing computers globally.

The cyberattack, known as Petya, froze the hospital's electronic medical record system early Tuesday, leaving doctors unable to review patients' medical history or transmit laboratory and pharmacy orders, said Rose Morgan, the hospital's vice president of patient care services.
Healthcare – Key Information Security Statistics

Budget
- 72% of healthcare organizations spend between 1%–6% of IT budget on information security
- Only 11% spend comparable to financial services (10-12% of IT budget)
- 62% say security budgets have stayed the same or decreased

Staffing
- 13% of healthcare organizations employ no cybersecurity staff
- 40% do not employ a named security leader (e.g., CISO)

Risks
- Healthcare was the victim of 88% of all ransomware attacks in the U.S.
- In 2017, 477 breaches were reported to HHS/OCR, affecting 5.6M patient records
- Data breaches are estimated to cost the industry $6.2 billion annually
<table>
<thead>
<tr>
<th>Entity</th>
<th>Number of Affected Individuals</th>
<th>Type of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airway Oxygen of Michigan</td>
<td>500K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Women’s Healthcare Group of PA</td>
<td>300K</td>
<td>Hacking of desktop and server</td>
</tr>
<tr>
<td>Urology Austin</td>
<td>279K</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Pacific Alliance Medical Ctr.</td>
<td>266K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Peachtree Neurological Ctr. Of Georgia</td>
<td>176K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Tampa Bay Surgery Center</td>
<td>142K</td>
<td>Hacking of server – public posting</td>
</tr>
<tr>
<td>McLaren Medical Group</td>
<td>106K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Emory Healthcare</td>
<td>79K</td>
<td>Hacking of server - extortion</td>
</tr>
<tr>
<td>Salina Family Healthcare Ctr.</td>
<td>77K</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Stephenville Medical &amp; Surgical</td>
<td>75K</td>
<td>Unauthorized disclosure/email</td>
</tr>
<tr>
<td>ABCD Pediatrics</td>
<td>55K</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Torrance California Medical Ctr.</td>
<td>46K</td>
<td>Hacking of email</td>
</tr>
<tr>
<td>St. Marks Surgical Ctr. in Florida</td>
<td>33K</td>
<td>Hacking of server</td>
</tr>
</tbody>
</table>
CIS Security Controls

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises
Healthcare Industry – Recommendations

- The healthcare industry seeks,
  - Support from the federal government to assist with protecting the industry from cyber risks, including:
    - Increased information-sharing activities specific to the healthcare industry that provide actionable information and defensive strategies on active cyber threats; and
    - A technical assistance center for smaller healthcare providers, which could provide guidance on how to protect, detect and recover from cyber events.
  - Flexibility from Congress to allow specific protections from Stark and Anti-Kickback penalties for hospitals that want to provide support to community physicians struggling with cybersecurity.