HCCA Compliance Institute
Boston, MA
2019

Blockchain Technology: Move Fast and Break Things Reconsidered

Scott A. Streibich, MBA, MHS, CHRC, CBE
Director, Research Compliance Operations
Johns Hopkins Medicine

Objectives

- Learn how blockchain technology operates and understand the implications for regulatory compliance related to patient information access, privacy and data retention
- Take away a risk asessment framework to share in your organization to educate others involved in blockchain development and adoption before problems arise

"Move fast and break things. Unless you are breaking stuff, you are not moving fast enough." *--In an interview with Business Insider's Henry Blodget*

"It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good" – *Congressional testimony, April 9, 2018*

HOME › COMPUTING › HEALTH APPS CAUGHT SHARING PERSONAL DATA WITH FACEBOOK

Health Apps Caught Sharing Personal Data With Facebook

By David Cardinal on February 25, 2019 at 7:30 am | 6 Comments

66 SHARES

HCCA
Compliance Institute
April 7–10 · Boston
Healthcare compliance strategies
Industry connections
Professional development
Register now ▶

Forbes Billionaires Innovation Leadership Money Consumer Industry Lifest

4,259 views | Feb 21, 2019, 04:02am

Zuckerberg Eyeing Blockchain For Facebook Login And Data Sharing

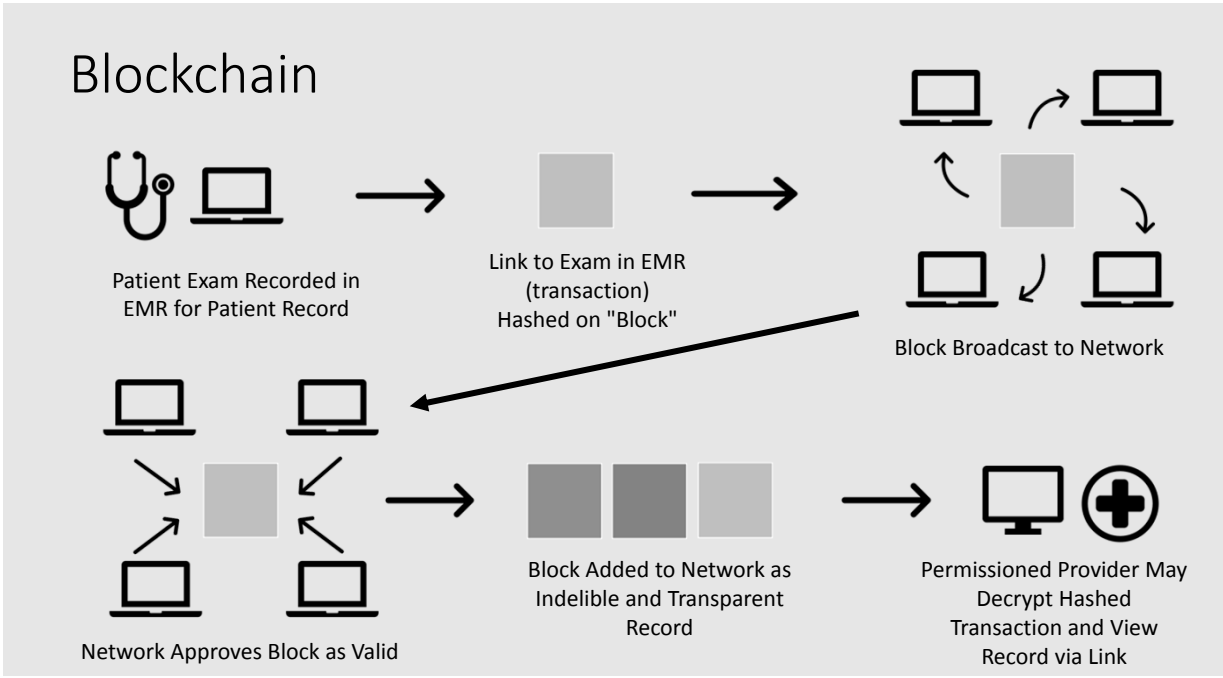
Darryn Pollock Contributor
Crypto & Blockchain

Blockchain

From "Blockchain: Opportunities for Healthcare," Deloitte Consulting August 2016

- A shared, immutable digital record of peer-to-peer transactions
- Cryptographic techniques allow participants to interact (e.g. store, exchange, and view information) without preexisting trust
- No central authority; instead transaction records are stored and distributed across all network participants
- Interactions with the blockchain become known to all participants and require verification before information is added, enabling trustless communication

Blockchain



Smart Contracts

Advantages

- Accuracy
- Speed
- Zero or Minimal Disputes
- Archival Record
- Resist Bias and Manipulation

Pitfalls

- Difficult to correct
- Cannot quantify "good faith dealing"
- Struggle with complex terms and conditions
- Need lawyers who code or coders who are lawyers
- Dispute resolution methods need validation (e.g. voting)

Best Use Cases for Blockchain

Tamper Prevention/Notice

- When a dataset has changed
- Proof of authenticity

Decentralization

- Avoidance of a central authority
- Control over the data to across the network

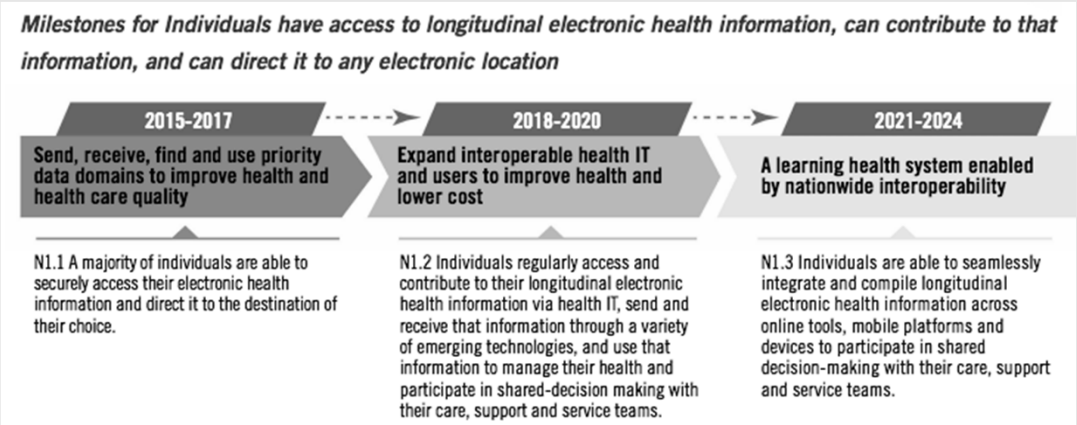
Transparency

- Parties involved lack preestablished trust
- Trust established through records visible to all participants

Critical Mass & Why Now

- Providers and existing EMRs are critical for launching any blockchain
  - FHIR
  - Project Argonaut
- Consumer Mediated Exchanges Could Become Reality
  - Existing exchanges are chiefly provider governed and directed
  - Offer limited or no patient directed release of information other than "opt out"

Nationwide Interoperability Roadmap



https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

Key Security & Privacy Risks

- HIPAA & Inclusion of Patient Data on the Blockchain
- Federal and State Law Concerning Presence of Sensitive Patient Data on the Blockchain
  - e.g., opioids
- Jurisdictional Elements Governing Blockchain Data
- GDPR, Personal Data and Rights on the Blockchain
- New Technology "First Mover" Challenges

HIPAA, Patient Data & Blockchain

- Identity Verification of Business Associate (blockchain provider) by Covered Entity
  - Spoofing attack
- Use
  - Blockchain cannot determine intent
- Minimum Necessary
  - Patient permission could be either too broad or too narrow to be useful or compliant

Additional Federal & State Regulations on PHI

- Substance Abuse 42 C.F.R. Part 2 (Part 2) Release Restrictions
- State Laws on HIV/AIDS, Mental Health, Alcohol Abuse Require Granularity or Specific Forms

Jurisdiction Challenges

- Blockchains Without Borders
- Build in GDPR Compliance Up Front?
  - Existing Guidance
- Consider Adopting Regulation from Blockchain and Privacy Pioneer States
  - California
  - Delaware
  - Ohio
  - Arizona
  - Tennessee

GDPR, Patient Data & Blockchain

- Right to Mask/Erase Personal Data from Publicly Accessible Searches or Databases
- Are these future best practices or mandates?

GDPR Specifics

Data Controller for Blockchain

- When participant is a natural person and the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal)
- When participant is a legal person and they register personal data in a blockchain
  - Wearables and Internet of Things (IoT)

Data Processor for Blockchain

- Smart contract developers who process personal data on behalf of the data controller

https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

GDPR Specifics

Presentation of Personal Data in Blockchain

- Commitment
- Hashing
- Cyphertext
- After a DPIA, justifed and residual risks minimzed
  - Hashed w/out key
  - Cleartext

https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

GDPR Specifics

Impact of rights on risk analysis

- Right of Access
- Right to Portability
- Right to Erasure
- Right to Rectification
- Right to Object to Processing

https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

Risk Assessment Methodology

- Risk Assessment Process
- Risk Model
  - Terms, Factors, Relationships
- Assessment Approach
  - Quantitative, Qualitative, Semi-Qualitative
- Analysis approach
  - Threat Oriented, Asset/Impact-Oriented, or Vulnerability-Oriented

Assessment Approach for Blockchain

Quantitative

- Availability, integrity and confidentiality
- Complex without automated tool
- Subjective assigment of risks with values provides false impression of specificity

Qualitative

- Probability / Consequences Matrix
- Good when $ cost of threat is not obvious
- May be difficult to categorize effectively

Qualitative Assessment

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	Supplementary Issue	Issue	Unacceptable	Unacceptable	Unacceptable
	Probable	Acceptable	Supplementary Issue	Issue	Unacceptable	Unacceptable
	Possible	Acceptable	Supplementary Issue	Issue	Issue	Unacceptable
	Unlikely	Acceptable	Acceptable	Supplementary Issue	Supplementary Issue	Issue
	Rare	Acceptable	Acceptable	Acceptable	Acceptable	Issue

Qualitative Assessment

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	Network Node DOS				
	Probable			Identity Spoofing		
	Possible		Loss of Pwd & Regeneration	Poorly written SmartContract	Malicious SmartContract	Tokens Banned
	Unlikely		Participant Withdraws	Regulatory Restrictions	Patient Loses Private Key	
	Rare				Cracking Hashed Pwds	51% Attack

Summary

- Blockchains are complex . . . proceed with caution
- Use cases may be incompatible with existing privacy and security regulations
- Risk assessments should include those partners bring to venture (e.g. Facebook, Apple)
- Access and transparency of public blockchains are very attractive to large scale hackers
- Qualitative assessment combined with threat-oriented analysis works well for new, complex technology