Take Aways from Session

• What controls (and legal requirements) must be considered
• Why current controls are insufficient
• Why administrative safeguards is not enough
• What considerations should be made for technical safeguards
• How does blockchain fit it
Why this is important now

• Many of the building blocks leveraging Blockchain based technology are there – these need to be assembled to form your next generation data security fabric

• Innovation is not a luxury – it is a must have in this fast paced moving information business environment
HIPAA and Research Basics
General Rule

• The HIPAA Privacy Rule lays out how protected health information may be used or disclosed by covered entities for research purposes.

• Research is “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” See 45 CFR § 164.501.

• Covered entities may always use or disclose for research purposes health information which has been de-identified
Privacy Protections & Research

• The Privacy Rule says how individuals must be informed of uses and disclosures of their protected health information for research purposes.

• For research, the Privacy Rule protects the privacy of individually identifiable health information and allows access necessary to conduct medical research.

• Most research involving human subjects falls under the Common Rule or the FDA human subject protection regulations that are similar to, but separate and distinct from, the Privacy Rule’s provisions for research.

• These human subject protection regulations include protections to help ensure the privacy of subjects and the confidentiality of information.

• **BUT** Privacy Rule builds upon these existing protections and establishes equal standards of privacy protection for any medical research.
With or without Authorization

• In order to obtain, create, use, and/or disclose individually identifiable health information for research, covered entities can do so
  • with individual authorization, or
  • without individual authorization under limited circumstances

• For research without an authorization, must have formal documentation of:
  • IRB or Privacy Board approval date of the alteration or waiver of authorization;
  • IRB or Privacy Board approval statement that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Privacy Rule;
  • A brief description of the protected health information;
  • A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
  • The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.
Criteria for Approval

- The use or disclosure creates only minimal risk to the privacy of affected individuals because:
  - researcher has adequate protections for any identifiers regarding improper use and disclosure;
  - researcher will destroy the identifiers at the earliest opportunity, unless a health or research justification exists for retention or is required by law; and
  - researcher provided adequate written assurances that the protected health information will not be reused or further disclosed

- The research could not practicably be conducted without the alteration or waiver of authorization; and

- The research could not practicably be conducted without access to and use of the protected health information.
Remote Access Preparatory to Research

• Remote Access
  • secure connections with access controls and authentication
  • Limited printing, downloading, copying, saving, data scraping (all would be removal)
  • transmission of electronic PHI

• Researcher outside the covered entity cannot control or retain the PHI

• Downloading permitted to the extent of viewing though the remote access, but limiting full retention
Remote Access Preparatory to Research

• Covered entities can rely upon representations of researchers, if reasonable

• Covered entities must assess risk of PHI removal by researcher (both from an administrative – trust of researcher’s representations – and technical – ability of research to actually retain PHI – standpoint and document inherent risks.

• Must be done on case-by-case basis
Limited Data Sets

• A limited data set **excludes specified direct identifiers** of the individual or other persons

**Controlled through a Data Use Agreement:**

• Puts forward specific permitted uses and disclosures of the limited data set matched to the purposes of the research

• Limits who can use or receive the data; and

• Require the researcher to agree to the following:
  • Only use or disclose as permitted by the data use agreement
  • Apply appropriate safeguards
  • Report any use or disclosure not allowed
  • Ensure everyone with access agrees to the same restrictions and conditions, and
  • Not try to identify the information or contact the individual.
Authorized Use and Disclosure

• More flexibility is possible when authorization from the individual is acquired

• Unlike other authorizations, a research authorization can make clear that it does not expire, it has no expiration date or event, or it continues until the “end of the research study”

• May be combined with
  • a consent to participate in the research
  • an authorization for a different research activity, provided that, if research-related treatment is conditioned on one authorization, the compound authorization must clearly differentiate and allow opt in to the unconditioned research activity.

• Future research purposes permitted, so long as the authorization adequately and reasonably describes the future research consistent with the individual expectations
**Authorized Use and Disclosure**

- New authorization guidance under the 21st Century Cures Act
- Congress wanted streamlined process to encourage data for research
- HIPAA-compliant authorizations must
  - be in plain language
  - contain specific information
    - a specific and meaningful description of the information
    - identification of those authorized to disclose and receive the information
    - description of each purpose of the requested use or disclosure
    - expiration date or expiration event that relates to the individual or the purpose
  - notice of all of the following:
    - the individual’s right to revoke the authorization in writing
    - any exceptions to the right to revoke
    - a description of how to revoke (or reference to NOPP)
    - ability or inability to condition treatment, payment, etc. on authorization
    - potential for redisclosure by researcher (and no longer be protected under HIPAA)
Authorized Use and Disclosure

Sufficient Purpose Descriptions
• Each purpose requested
• Sufficient for individual to make choice
• Not necessarily each future research, but enough to understand
• Look to “could one reasonably expect such

Expiration of Authorization
• On future research
• If purpose was “research repository” for ongoing use:
  • “None”
  • “End of Research”
• Revocation
  • From revocation forward
  • Previous use allowed
  • “Reminders”
Democratizing Data Access - Blockchain and Healthcare: Better Health Information Sharing

NCHICA
June 3, 2019

Shay Hassidim – Sema4 CTO & CISO
shay@sema4.com
Shay Hassidim  
CTO & CISO  

- 25 years in Enterprise SW  
- DevOps, SecOps, ITOps, Database, Big data, HPC, ML, IMC, Cloud, IoT, CyberSecurity  
- Healthcare, FiS, Logistics, Telecom, eCom, Gaming, Homeland security  
- Past Life - Products / OSS Projects:  
  - Sirius DBMS – EMR database  
  - Versant ODBMS  
  - GigaSpaces XAP – IMC, OSS  
  - GigaSpaces Cloudify – CMP, OSS
Sema4 vision

We are a patient-centered predictive health company founded on the idea that more information, deeper analysis, and increased engagement will improve the diagnosis, treatment, and prevention of disease.

We believe the best way to promote wellness is to understand humans holistically, as systems akin to vast information networks.
Sema4: Patient-centered predictive health company

- Spun out of Mount Sinai, a premier research and patient care organization and one of largest healthcare systems in US, in 2017
- **Interdisciplinary team** of scientists, data engineers, and clinicians, transforming future of healthcare through *data-driven insights*
- One of **largest clinical genomics labs** in world
  - >150,000 tests run/year
- Founded on idea that more information, deeper analysis, and increased engagement will *improve diagnosis, treatment, and prevention of disease*
Security Game Plan
IT Resources Security Guiding Rules

Visibility and assessment

Accountability & responsibility

Organize resources - Segmentation and isolation

Continuous sample, detect and respond cycle

Policy enforcement - Proactive, Reactive

Education, awareness and culture

Prepare a crises response plan
Each layer generating hundreds of data points every second. Impossible to manage via humans to enforce company and industry policies (HIPAA, NIST, HITRUST/CSF...).
Data Access Control Challenges
Data Access - Challenges

- **Cloud A**
  - On-Prem/Cloud data services access policies

- **Cloud B**
  - On-Prem/Cloud virtual network & storage ACL

- **On-Prem**
  - On-Prem/Cloud physical network & storage ACL

- **IT Internal - A mesh of cloud native policies, custom policies (user, service, roles) with interconnectivity between different physical and virtual networks, human/machine/virtual users, PHI/Non-PHI data sets**

- **Challenges**
  - No unified data Access control layer
  - Every On-Prem/Cloud resource require different access control system
Typical Cloud Organization – Multi account Structure

Each one of these is a separate cloud account with its own specific IAM groups, users, policies, buckets, security groups, and more.
Typical Cloud Organization – Multi account Structure

**PHI vs Non-PHI**

Each one of these is a separate cloud account with its own specific IAM groups, users, policies, buckets, security groups, etc.
Typical Cloud Organization – Multi account Structure

**PHI vs Non-PHI – Hierarchical Org Unit Management**

Each one of these is a separate cloud account with its own specific IAM groups, users, policies, buckets, security groups...
Change Control & Configuration Management

On-boarding, off-boarding, specific dev requests

IT Admin AWS CLI

Eye In the Sky
Surveillance and auto-remediation system

IT Policies (code)

• AWS account creation and preparation for use
• User account creation/deletion/deactivation - specific AWS account(s), All org accounts
• User account access keys creation/deletion/deactivation - specific AWS account(s), All org accounts
• Key pair creation/deletion - specific AWS account(s), All org accounts
• Bucket, Volumes, Snapshot management
• VPC, Security Group (FW) management

AWS
Standard IAM Groups Permissions

- **Service** – Ability to assume roles for a limited duration leveraging a specific permissions policy/role
- **Dev** – Access to all typical dev resources. Access to PHI accounts requires MFA.
- **Admin** - Access to all typical dev resources with admin access. Access to PHI accounts requires MFA.
- **Super User** – IAM access. Ability to manage users and access keys
- **Full Access** – root user – Account level permissions
Assume Role

**Step 1.** Limited long-term credentials to call the AWS Security Token Service (STS) AssumeRole API, specifying the ARN for the role S3 role.

**Step 2.** AssumeRole request using Policy ARN & session name. Response returns temporary security credentials for the IAM role.

**Step 3.** Make AWS API call using the temporary security credentials returned in the previous step.

Role Permissions policy:
```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Deny",
      "Action": "s3:PutObject"
    },
    {
      "Sid": "VisualEditor2",
      "Condition": {
        "StringNotLike": {
          "aws:userid": "POLICY-1D:SessionName"
        }
      }
    }
  ]
}
```

Role Trust Policy:
```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccoutID:username"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```
Data Access Control Solution
Universal Data Access Control

Single Pane of Control

A SINGLE CONTROL POINT FOR ALL DATA

Cloudian
NAS
CIFS
FTP
DropBox
OpenStack
SharePoint
Salesforce
Office 365
Google Drive/Storage
Amazon S3
Azure

For USERS
Collaborate, manage, search and share data across all cloud services securely

For IT
✓ Manage cloud sprawl / shadow IT
✓ Audit and track shared files
✓ Set File Sharing Policies
✓ Search across all storage services

Cloud Control protection fabric for files

Security and Protection
Data Access Control – Phase I

Universal Access layer

On-Prem/Cloud data services access policies

On-Prem/Cloud virtual network & storage ACL

On-Prem/Cloud physical network & storage ACL

- One Standard data Access layer via UI / API / CLI / Native OS tools
- Abstracting / Hiding cloud/on-prem data security layer complexity
- One standard data discovery and classification identify PHI/PCI

IT Internal - A mesh of cloud native policies, custom policies (user, service, roles) with interconnectivity between different physical and virtual networks, human / machine/virtual users, PHI/Non-PHI data sets
Data Access Control Phase II

Universal Access layer

Blockchain based permission-ing system

On-Prem/Cloud data services access policies

On-Prem/Cloud virtual network & storage ACL

On-Prem/Cloud physical network & storage ACL

Democratized Data access layer

• One Standard data Access layer via UI / API / CLI / Native OS tools
• Abstracting / Hiding cloud/on-prem data security layer complexity
• One standard data discovery and classification identify PHI/PCI

IT Internal - A mesh of cloud native policies, custom policies (user, service, roles) with interconnectivity between different physical and virtual networks, human/machine/virtual users, PHI/Non-PHI data sets
Classic Healthcare Blockchain ecosystem

Member

Healthcare Big Data Company

Local/International National Genomics institutions

DNA, EMR Biometric data

Pharma

Medical care org

Rx

Pharmacy

Clinical laboratory

Insurance co.
Data Access Control Working example
Estonian Health Information Sharing Model

Patient’s explicit consent is not needed for recording nor sharing the data. Patient have the right to hide the data

Estonian Health Information Sharing Model

98% drop with paperwork and bureaucracy!

- 97% of patients have countrywide-accessible digital records
- 99% of prescriptions are digital
- 99% of public services online with 24/7 access
- The electronic ID-card system and blockchain technology are used to ensure health data integrity and mitigate internal threats to data. In use since 2012.

Healthcare 4.0 is Estonia’s solution for the future.

By leveraging personalized medicine and genome-based analysis, people will become more aware of the factors influencing their health, and individuals will take more responsibility for managing their own health.

Patients will be able to access information wherever they happen to be at a time of their choosing, enabled by point-of-care devices – equipment provided by the state that patients may use themselves.

Estonia will provide global health accounts and introduce the benefits of medical procedures based on artificial intelligence.
Lessons Learned

Think long term

Get buy in from the upper management

Adjust policies and enforcement tactics based on organization business goals

Run frequent education sessions
Thank You