Members of the Confidentiality Coalition

AdvaMed
AdventHealth
America’s Health Insurance Plans
American Hospital Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
athenahealth
Augmedix
Baxter
Biogen
Blue Cross Blue Shield Association
BlueCross BlueShield of North Carolina
BlueCross BlueShield of Tennessee
Cerner
Change Healthcare
CHIME
Cigna
Ciox Health
City of Hope
CLEAR
Cleveland Clinic Foundation
College of American Pathologists
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
EMD Serono
Epic
Express Scripts
Fairview Health Services
Federation of American Hospitals
Genentech
Genetic Alliance
Genosity
Guardant
Healthcare Leadership Council
Health Management Systems
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Labcorp
Leidos
Mallinckrodt
Marshfield Clinic Health System
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Millennium Health
Memorial Sloan Kettering Cancer Center
Merck
MetLife
National Association of Chain Drug Stores
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University HealthSystem
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
SCAN Health Plan
Senior Helpers
SSM Health
State Farm
Stryker
Surescripts
Teladoc Health
Texas Health Resources
The Commons Project Foundation
Tivity Health
UCB
UnitedHealth Group
Vineti
Vizient
Workgroup for Electronic Data Interchange
ZS Associates
ARTIFICIAL INTELLIGENCE, HIPAA & BEYOND

Joe Ashkouti
Chief Privacy Officer
Change Healthcare

07.15.2020
Agenda

1. Artificial Intelligence (AI) vs. Machine Learning (ML) and Deep Learning

2. The Healthcare “Industry” and HIPAA

3. The Role of a Business Associate like Change Healthcare in using AI/ML

4. Training AI/ML with HIPAA covered data

5. Standards needed to create Transparency and Explainability in the development and use of AI/ML

6. Standards needed to address Ethical issues and eliminate Bias, Disparate Impact, and Discrimination in AI/ML
Artificial Intelligence (AI) - Machine Learning (ML) - Deep Learning (DL)

(Businesses in healthcare primarily use ML and DL)

Artificial Intelligence – machines being able to carry out tasks in a way we would consider as exhibiting human intelligence (Narrow vs. Generalized AI)

Machine Learning – an approach to achieve AI based on the idea that we should be able to give machines access to data and let them learn for themselves

- Uses algorithms to parse data, learn from it, and make predictions about something in the world
- No hand-coding software routines with a specific set of instructions to accomplish a task; instead, the machine is “trained” using large amounts of data to learn to perform the task

Deep Learning – a technique using machine learning like the neural network of the human brain and works on a system of probability

- The system is fed a lot of data (in one case 10 million YouTube videos), which it can use to make decisions about other data, and is able to make statements, decisions or predictions with increasing degrees of certainty
- “Deep” means that, as the network gains more experience, it can increase its probability of a correct classification, and learn from its mistakes

Sources: Forbes Blogs by Jeff Caitlin October 2017 and Bernard Marr December 2016, and NVIDIA blog by Michael Copeland July 2016
Hotels/Lodging is an industry. Healthcare is not.

**Healthcare is:**

- A conglomeration of industries and actors – e.g., payers (insurance companies), physicians, health systems, service providers, and government that must co-exist in order to provide care and to get paid for it; and

- Brought together by laws and their implementing regulations – e.g., Health Insurance Portability and Accountability Act (HIPAA) and its Privacy and Security Rules

HIPAA creates a common privacy architecture to develop Artificial Intelligence (AI) / Machine Learning (ML) for disparate industries within "healthcare", but:

- HIPAA did not contemplate Artificial Intelligence and Machine Learning (AI/ML), e.g., use of PHI to train AI/ML models vs. de-identified data, and the need for large amounts of data vs. the "minimum necessary standard";

- There are no standards for Transparency or Explainability when AI/ML is making decisions in a regulated environment, e.g., for patients, customers and government regulators; and

- Covered Entities sometimes use Business Associates who have more experience in AI/ML than in healthcare and HIPAA privacy
Mission-Critical Partner to the Healthcare Industry

- **33,000 Pharmacies**
- **900,000 Physicians**
- **118,000 Dentists**
- **600 Laboratories**
- **5,500 Hospitals**
- **2,200 Payor Connections**
- **3,300+ Facilities using Imaging Solutions**
- **$1 Trillion Healthcare Claims**
- **14 Billion Healthcare Transactions**
- **1 in 3 U.S. Patient Records**
- **2,200 Payor Connections**

Leading analytics franchise
Pervasive network providing insights
Leading payor & provider relationships

- Improve clinical decision making
- Simplify billing, collection and payment
- Enable a better patient experience
- Reduce administrative errors
- Increase cash flow and lower costs
- Enhance transparency
Artificial Intelligence/Machine Learning: Helping Meet Market Changes

Change Healthcare uses AI/ML to reduce waste, increase efficiency, and help payers and providers meet market changes.

**Wasteful Spending**
- U.S. healthcare expenditures expected to grow from $3.5T in 2017 to $5.7T by 2026
- 30% of U.S. healthcare spending is estimated to be wasteful

**Growth of Higher Risk Patient Populations**
- 41% enrollment in Medicare Advantage by 2027
- > 65 population growing 34% annually (3-5x HC spend vs < 65 population)

**Shift to Value-Based Care**
- Model shifting to incentivize value and quality
- Need for enhanced documentation, robust data and sophisticated analytics

**Increasing Consumerism**
- HDHPs have grown 12% annually since 2012
- Need for personalized solutions and cost, quality, transparency and decision support tools

**Proliferation of Healthcare Data**
- Unprecedented rise in HC data (>2,300 exabytes by 2020)
- Solutions needed to utilize data and identify insights that improve outcomes and decrease costs

Source: National Academy of Medicine; Office of the Actuary; U.S. Census Bureau; Congressional Budget Office; America’s Health Insurance Plans; Centers for Medicare & Medicaid Services
Training AI/ML needs large amounts of data (PHI vs. De-identified Data)

Training by Covered Entities (CEs) vs. Business Associates (BAs)

Protected Health Information (PHI) – we believe training an AI/ML algorithm is a "use" of PHI under HIPAA, but...

- △ HIPAA does not address AI/ML directly, and the Office for Civil Rights within HHS has not yet issued any guidance
- △ CEs can use their own PHI to train AI/ML and create new products/services but may not have the coding experience. Also, without access to other CEs' data the AI/ML algorithm’s decision-making may be skewed or exhibit inherent bias
- △ BAs cannot use PHI for product development. BAs may be able to use PHI from multiple CEs to provide more accurate AI/ML services and limit bias, but BAs have material use restrictions imposed by HIPAA and by CEs through contracts

De-identified PHI – de-identified data may be used to train AI/ML and create new products and services, but...

- △ CEs may de-identify their own data to train AI/ML, but may need to license additional de-identified data sets to achieve more accurate outcomes
- △ A BA may de-identify PHI on behalf of its CE customers to create larger, more accurate data sets only if its CE customers grant the BA those rights in writing

Minimum Necessary – business needs guidance on how to reconcile HIPAA’s minimum necessary rule with AI/ML’s need for large amounts of data for it to learn, improve its accuracy, and eliminate bias
Standards for Transparency and Explainability are needed to develop and accelerate the use AI/ML across healthcare

- **Transparency and Explainability** are approaches to building AI/ML that allow humans to observe and understand how the AI/ML model makes decisions.

- Healthcare entities are sometimes reticent to adopt AI/ML services because of a lack of Transparency and Explainability about how the machine made its decision (even for non-treatment related decisions).

- Consider the examples of Transparency and Explainability to patients and to regulators:
  - **Patients** – AI/ML could be used to make decisions about a patient’s eligibility for insurance. What if she was denied coverage inappropriately? In the EU, individuals have the right to know when AI/ML is making a decision about them and the right to contest the decision if they think the decision is incorrect.
  
  - **Regulators** – most tasks in healthcare are regulated. For example, over-billing Medicare can lead to False Claims Act liability. If a regulator thinks a provider is over-billing and AI/ML is used to create the bills, the provider and the AI/ML creator must be able to explain how the AI/ML made the billing decisions in question and whether there was any human oversight.
Only a few Standards address Ethics, Bias, Disparate Impact, Discrimination in AI/ML

- **Department of Defense** created ethical principles for the use of AI: Responsible, Equitable, Traceable, Governable, and Reliable

- **Consumer Technology Association** created ANSI accredited standard for AI/ML in healthcare

- **National Institute of Standards and Technology (NIST)** is working on “appropriate technical standards” for AI/ML

- **Institute of Electrical and Electronics Engineers (IEEE)** created a policy and standards statement called “Ethically Aligned Design” for the creation AI/ML that prioritizes human well-being
Industry, Government and Joint Initiatives are needed to accelerate the development and use of AI/ML across “Healthcare”

1. OCR Guidance on complying with HIPAA when developing and using AI/ML by a Business Associate or a Covered Entity (similar to OCR’s cloud computing guidance)

2. Guidance/Standards to provide Explainability and Transparency when AI/ML is used by or for healthcare stakeholders

3. Guidance/Standards to address Ethical issue and eliminate Bias and Discrimination in AI/ML
BEYOND HIPAA

Diane Sacks, Esq.
Counsel to Confidentiality Coalition
July 15, 2020
At Time of HIPAA Enactment in 1996

Entities Subject to HIPAA
- Health plans
- Health care clearinghouses
- Health care providers that performed certain data exchanges electronically
- Business associates (service providers) of the above

Entities Not Subject to HIPAA (unless also one of the above)
- Employers
- Pharmaceutical manufacturers and their patient assistance programs
- Medical device companies
- Health care providers that don’t perform certain data exchanges electronically
- Researchers
What has Changed Since 1996?

- **in non-HIPAA entities** collecting personal data
  - Internet-based data collection, such as search engines and social media platforms

- **in the volume** of personal data being collected by these entities
  - New technology allowing analysis of vast quantities of data

- **in the health-related** or sensitive nature of the data
  - Health-related apps such as fitness, diet, heart rate, glucose, personal health record apps
Recent Developments Highlight Challenges

- Contact-tracing apps for COVID-19
  - Data collection by employers, governments, technology companies, other non-HIPAA entities

- CMS & ONC interoperability rules (published May 2020)
  - Require HIPAA entities to share patient records and claims data through standardized APIs with third-party (non-HIPAA) apps at patient’s direction
What are the Concerns?

- No comprehensive national privacy law or standards in the United States
- Consumers often don’t know when HIPAA applies and when it does not
  - E.g. a doctor recommends that a patient using a specific health monitoring app
- Consumer trust underpins the essential flow of health data in health system
- Consumer trust is eroded as more health data falls outside the protections of HIPAA, making consumers less willing to share the information needed to deliver quality care
What Should Privacy Standard for Non-HIPAA Entities Include?

- Robust privacy and security protections consistent with HIPAA, including:
  - Minimum necessary standards
  - Privacy notice/transparency requirements that explain privacy practices in simple, straightforward language
  - Breach notification and mitigation
  - Risk-based physical, technical and administrative safeguards
  - Individual data rights, such as to access, amend and, as appropriate, delete records
  - Written authorization required to use data for other purposes
  - Meaningful enforcement

- Harmonization with HIPAA principles, concepts and definitions
- Leave HIPAA ecosystem intact – it works!
- Uniform, national standards
Approaches in Recent Legislative Proposals

- General agreement on
  - Transparency/privacy notices
  - Data minimization
  - Data security/safeguards
  - Some individual data rights

- Differing approaches to permitted uses and disclosures
  - Consent-based models
  - Restriction-based models

- Differing approaches to enforcement
  - FTC and State Attorneys General
  - Private right of action
  - New data protection agency

- Disagreement on Preemption of State Laws
Diane Sacks, Esq.
dianesacks@sacksllc.com
202-459-2101