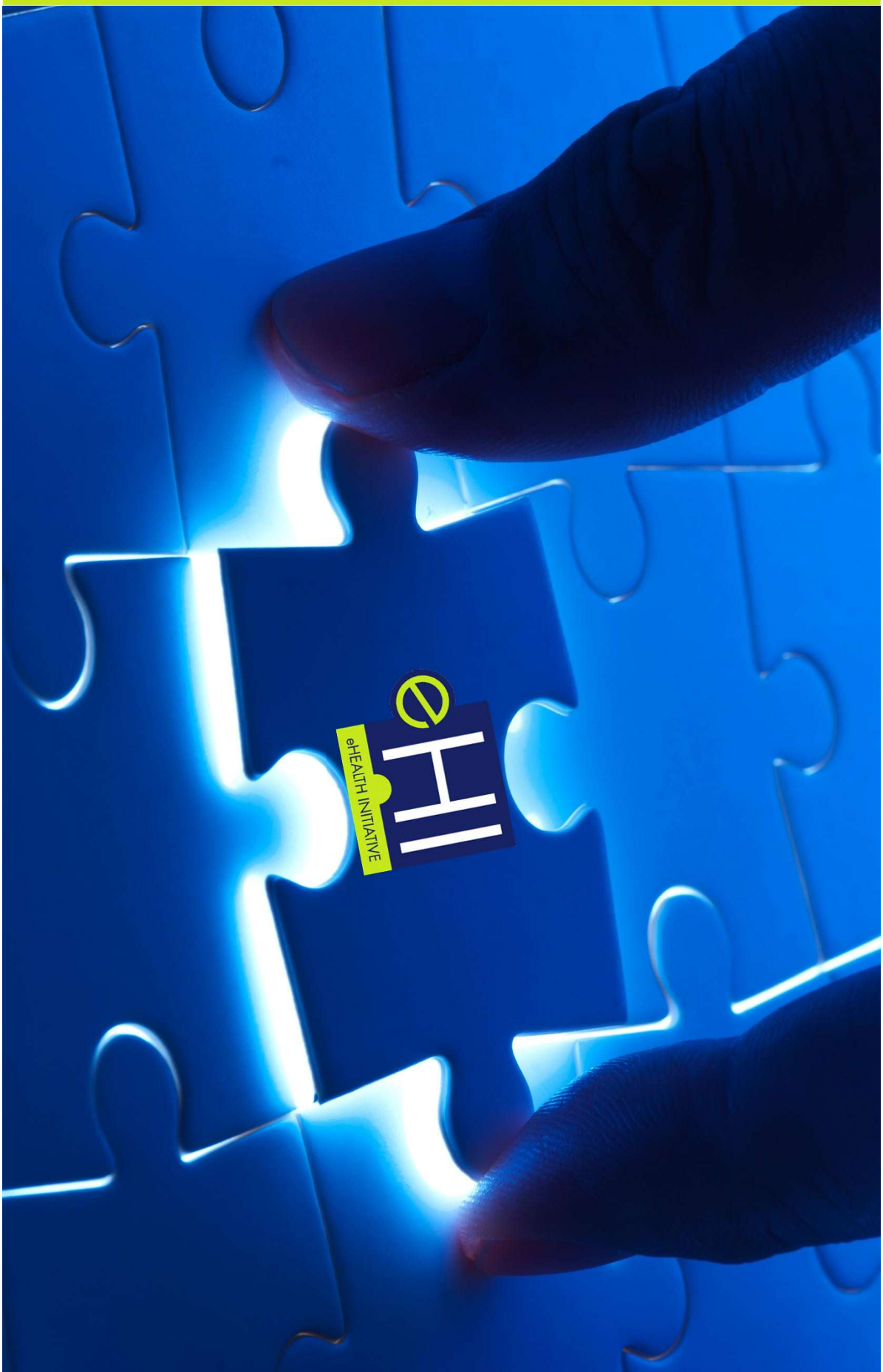
eHEALTH INITIATIVE



HIPAA for Dummies

February 6, 2020

2:00 – 3:00 p.m.

SPEAKER

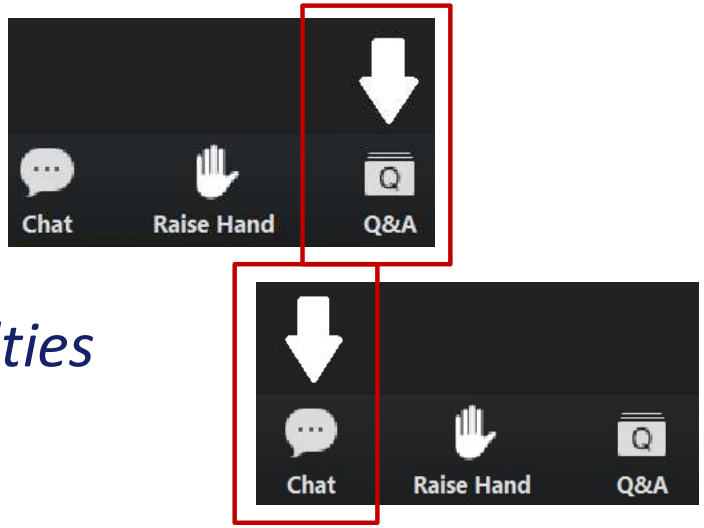
Alice Leiter, JD, Vice President & Senior Counsel, eHealth Initiative

Agenda

- **Welcome**
  - **Claudia Ellison,** Director of Programs and Services, *eHealth Initiative*
- **Presentation:**
  - **Alice Leiter, JD, Vice President & Senior Counsel,** *eHealth Initiative*
- **Q&A**

Housekeeping

- **All participants are muted**
- Use the **Q&A** box to ask a question related to the presentation
- Use the chat box is for *technical difficulties* and other questions / comments



Presentation slides are in the eHI resource Center
https://www.ehidc.org/resources

eHI's Mission

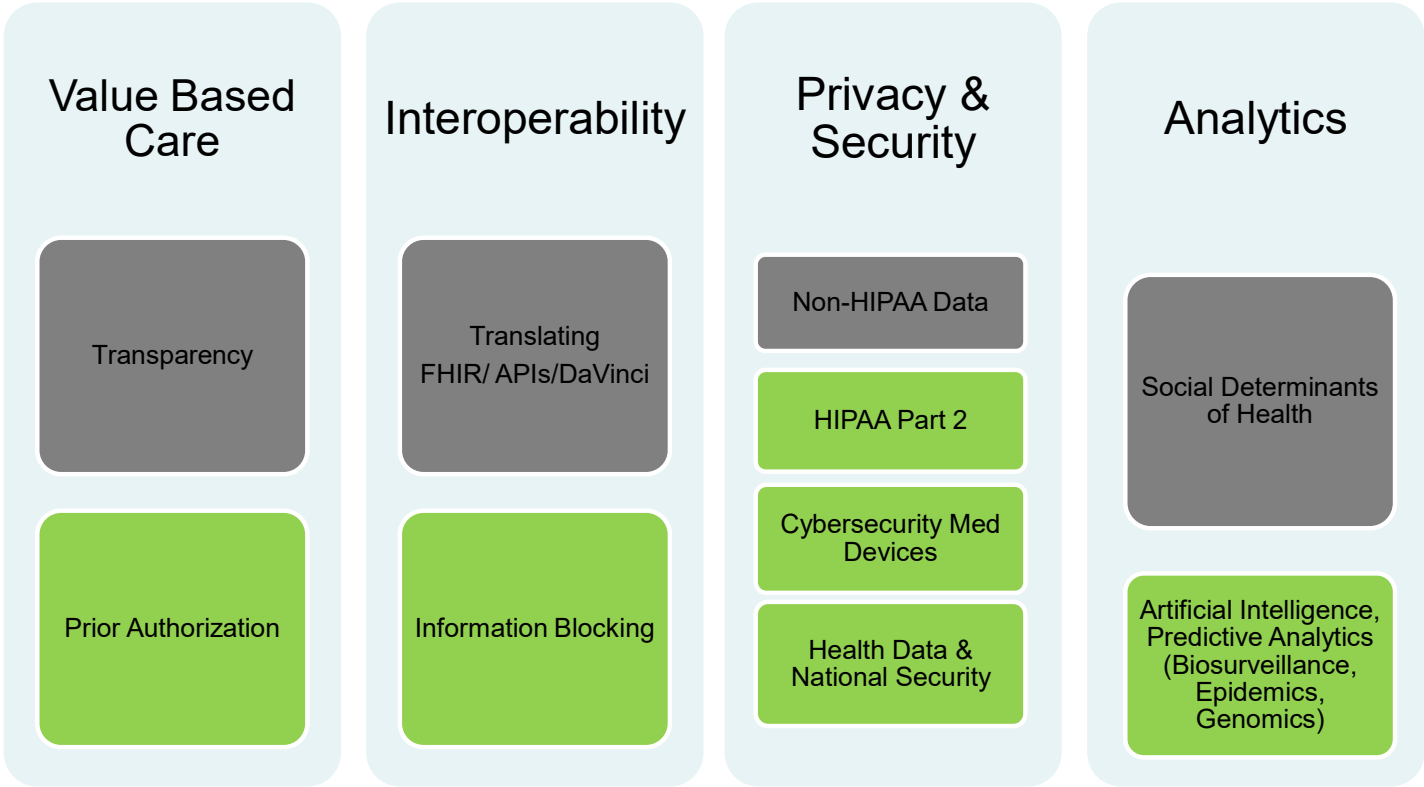
To serve as the industry leader in **convening executives** and multi-stakeholder groups to **identify best practices** that **transform healthcare** through the use of t**echnology and innovation**

eHI Leadership Council

Our Members


3M
4medica
ACOG
AHIMA
inovalon
InterSystems
Johnson & Johnson
KHN
Allscripts
American Academy of Family Physicians
American Cancer Society
ACR
LexisNexis
LifeWIRE
Lilly
MAEHC
American Heart Association
American Hospital Association
Anthem
Availity
manatt
Marshfield Clinic
Massachusetts Medical Society
Mayo Clinic
Booz | Allen | Hamilton
BayCare Health System
BDO United States
Bristol-Myers Squibb
Medicity
A Healthagen Business
National Alliance
NeHII
nextgen healthcare
CAQH
Cerner
CHANGE HEALTHCARE
CHRISTUS Health
noridian
Healthcare Solutions
Northwell Health
OhioHealth
BELIEVE IN WE
Pfizer
commonwell
HEALTH ALLIANCE
Cognizant
connective
CORHIO
Prescriptions for a Healthy America
pwc
verato
SHIEC
CRISP
DataFile
EHNAC
fitbit
SOLERA
Sonora Quest Laboratories
Strategic Interests
surescripts
How Healthcare Gets Connected
GLHC
Google Cloud
GUNDERSEN HEALTH SYSTEM
healthcurrent
THE HEALTH COLLABORATIVE
UnitedHealthcare
updox
VALIDIC
Healthix
healthwise
HL7
Hogan Lovells
verato
virence
welldoc
Wellmark
zipnosis
eHI
eHEALTH INITIATIVE

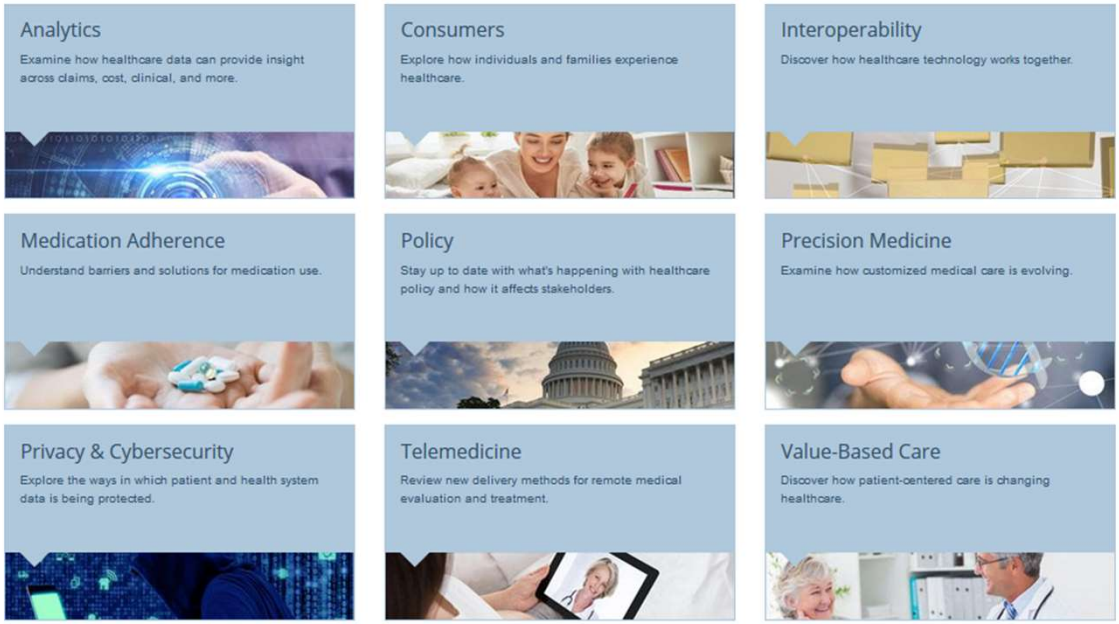
Current Areas of Focus



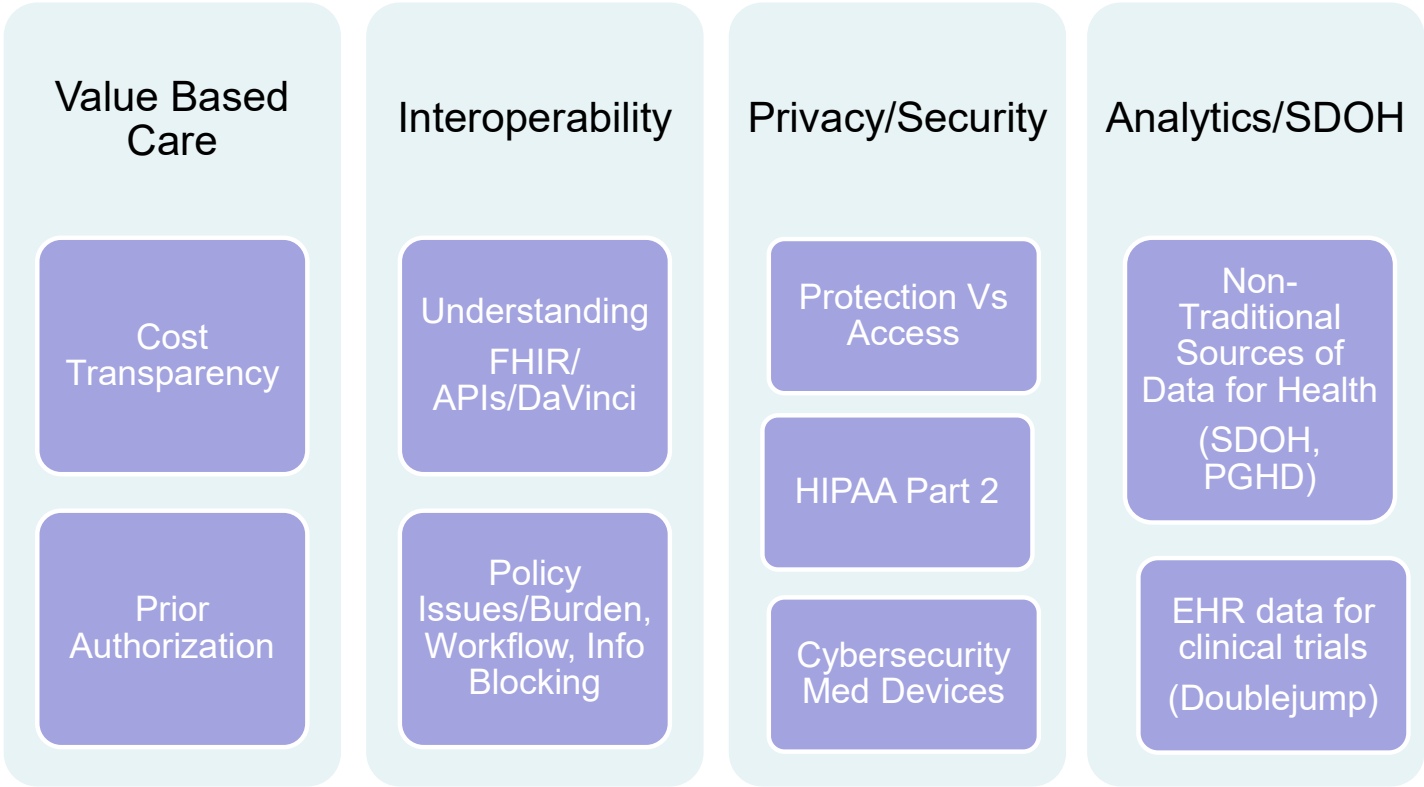
eHealth Resource Center

Thousands of Resources

- Best Practices
- Reports
- Surveys
- Policy Briefings
- Comment Letters



Current Areas of Focus



eHealth Resource Center
www.ehidc.org/resources

- eHealth Resource Center available with best practices & findings identifying and disseminating best practices
- Online Resource Center: Over 600 new pieces of content, 125 best practices added this year

HIPAA, Not HIPPO.

Two As, Not Two Ps

- Health Insurance Portability and Accountability Act
- Primary federal law protecting health information
- Governs the permissible uses and disclosures of health information that identifies the subject of the information
- Covers only information created, received or maintained by or on behalf of health care providers and health plans
- Often thought of as a restrictive law; actually quite permissive

Once Upon a Time…
HIPAA Statute (Public Law 104-191)

- Passed by Congress in 1996
- Designed to improve the efficiency and effectiveness of the health care system
- Aimed to modernize the flow of information as more of it became digital
- Among other things, required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge

The Juicy Stuff: HIPAA Regulations

1. **Privacy Rule**
   - Applies to providers (doctors), health plans (insurers) and health care clearinghouses (known as "*covered entities*") and their contractors (*"business associates")*
   - Sets limits and conditions on the uses and disclosures that may be made of protected health information (PHI) without patient authorization
   - Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections
2. **Security Rule**
   - Establishes a national set of security standards for protecting health information
   - Provides technical and non-technical safeguards that covered entities must put in place to secure individuals' electronic PHI

HIPAA Regulations

3. <u>Enforcement Rule</u>

- Newer – part of HITECH in 2009
- Strengthens civil and criminal enforcement of the HIPAA rules
- Significantly increased civil monetary penalties for violations
- Office for Civil Rights at HHS has responsibility for HIPAA violations

4. <u>Breach Notification Rule</u>

- Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI

Privacy Rule – Who and What Does it Cover?

1. **Covered Entity –** health care providers (doctors), health care plans (insurers), and health care clearinghouses
2. **Protected Health Information (PHI) –** *"Individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral

   → *"Individually identifiable" is broadly defined*
3. **Business Associate –** a contractor of a covered entity that performs services and handles PHI on its behalf

Privacy Rule – Who/What Does it NOT Cover?

- Data created or held by a person or company that is **not** a covered entity
- Data that is **not** individually identifiable

  → Data that has been de-identified is no longer covered by HIPAA

Privacy Rule – Who/What Does it NOT Cover?

- Data you generate is not covered by HIPAA (unless transmitted to a covered entity)

  →This includes most data on your computer or phone, like the info you upload into a calorie-counting app, a fitness tracker, or your order history on Amazon

  → Most apps and tech companies are not HIPAA covered entities in their own right

  →YOU are not a HIPAA-covered entity

- Once data leaves a HIPAA-covered entity, either for a required or permitted purpose, or because an individual authorized the disclosure, and goes to a non-HIPAA covered entity, the law and its protections no longer apply

Business Associates

- What are the types of things Business Associates do?
  - claims processing
  - data analysis
  - utilization review
  - billing
- Business Associate Agreement
  - When a covered entity hires a Business Associate to perform services on its behalf, the Privacy Rule requires that the covered entity include certain protections for the information in a *business associate agreement (BAA)*
  - BAAs have to specify precisely how the BA will and will not use CE data
  - Business Associates must follow the Privacy Rule, and follow the same rules as covered entities with respect to PHI

Uses and Disclosures Under the Privacy Rule

- In general, the Privacy Rule prohibits Covered Entities (and their Business Associates) from using or disclosing PHI, UNLESS:
  - (1) the Privacy Rule permits or requires such a use or disclosure; or
  - (2) the individual who is the subject of the information (or the individual's personal representative) authorizes the use/disclosure in writing

Permitted Disclosures of Health Data under HIPAA – "TPO" (without patient authorization)

- **Treatment**
  - Provision, coordination, or management of health care
  - Consultation between health care providers
  - Referral of a patient from one health care provider to another
- **Payment**
  - Various activities related to obtaining payment or reimbursement, obtaining premiums, providing benefits or determining coverage/eligibility
- **Health care operations** (broadest category)
  - Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment
  - Includes staff evaluations, case management and care coordination

Other Permitted Disclosures of Health Data under HIPAA (without patient authorization)

- Required by law
- Public health activities
- Victims of abuse, neglect or domestic violence
- Health oversight activities
- Law enforcement purposes
- Decedents
- Cadaveric organ, eye, or tissue donation
- Research
- Serious threat to health or safety
- Essential government functions
- Workers' compensation

How Does This Look in the Real World?

- "Project Nightingale" – the "secret" data-sharing arrangement between Google and Ascension Health
  - Just because consumers didn't know about it doesn't mean it was sinister
  - This type of relationship is both common and legal
  - Fully HIPAA-compliant – Google and Ascension signed a Business Associate Agreement that outlines the relationship between the two, companies, the purpose of the relationship, and what Google could and could not do with patient data
- There is always room for improvement, but public reaction to this "discovery" is more of an issue of transparency, awareness, and education

Coming Down the Pike

- CMS Interoperability rule
  - Would require insurers participating in CMS-run programs (Medicare, Medicaid, federal health insurance exchanges) to allow patients to instantly access personal health information electronically through FHIR-based APIs
- CMS Interoperability and "Data Blocking" Exceptions Rule
  - Hospitals and physicians participating in Medicare are required to make select information electronically available to patients using APIs
- API developers would not necessarily be subject to HIPAA or BAAs, creating a gap in patient privacy protections


Bedankt
谢谢您
Thank you!
Grazie
Danke
Merci
謝謝您
Takk
Obrigado
Gracias