Framing Our Work in 2019
PRIVACY
INTRODUCTIONS
30 SECOND EACH ICEBREAKER
Panelists

• Robert D. Belfort, Partner, Manatt Health

• Steve Kastin, MD, Senior Executive Advisor and Chief Medical Information Officer (CMIO), Booz Allen Hamilton
Our Work

• Publications
  • Capitol Hill Briefings
  • HHS, FDA, Leadership
  • Partnerships
  • Education Programs

• Surveys, Reports
  • Member Feedback
  • Expert Roundtables
  • Policy Steering Committee

PROMOTE
Best Practices & Solutions

ASSESS
Identify and Define Problems

INFLUENCE
Develop Recommendations
Guidelines

EDUCATE
Convene and Educate

• Guidelines, Roadmaps
  • Comment Letters
  • Expert Roundtables
  • Advisory Boards, Workgroups
  • Policy Steering Committee (PSC)

• Expert Roundtables
  • Capitol Hill Briefings
  • Webinars
  • Workshops
  • Linked In Forums, Townhalls, Twitter
Current Areas of Focus

(\textcolor{green}{Green} Addressed at Roundtables Today)

Value Based Care
- Cost Transparency
- Prior Authorization

Interoperability
- Understanding FHIR/ APIs/DaVinci
- Policy Issues/Burden, Workflow, Info Blocking

Privacy/Security
- Protection Vs Access
- HIPAA Part 2
- Cybersecurity Med Devices

Analytics/SDOH
- Non-Traditional Sources of Data for Health (SDOH, PGHD)
- EHR data for clinical trials (Doublejump)
Privacy and Security: Protection vs Access

• This initiative will develop policy recommendations regarding healthcare privacy state and federal laws that are negatively impacting consumer access to their healthcare data.

• Problem: The rise of consumer-facing health care websites, mHealth apps, and connected medical devices has raised new privacy and security challenges regarding the collection and sharing health data. The existing health information privacy regulatory framework, which is built around HIPAA and state privacy laws, was not designed for the rapidly changing digital landscape driving State and Federal agencies to develop regulations. Although the laws are designed to protect all involved, they can create barriers to exchange and access data. For example, the California Consumer Privacy Act introduces burdensome obligations, most of which were previously unseen by American companies and several of which present questions about implementation.

• Solution: eHI will identify the current regulations and determine how they both support consumer privacy and, at the same time, negatively impact access for consumers and other key stakeholders. eHI will propose policy recommendations and develop guidelines regarding current regulations for payers, providers, and vendors.
Key Data Sharing Issues Driving Regulatory Change

Robert Belfort
Manatt, Phelps & Phillips, LLP
Key Health Data Sharing Issues

- Increasing patients’ access to their own health information
- Eliminating barriers to data sharing within the health care system for treatment and care coordination
- Managing the rapid expansion of health data collection by technology companies outside the traditional health care system
Recent Legislative and Regulatory Activity

February 17, 2009
HITECH enacted

May 25, 2018
GDPR Effective

March 4, 2109
ONC and CMS Interoperability Rules Issued

December 13, 2016
21st Century Cures Act Enacted

June 28, 2018
CCPA Enacted
Historical Obstacles to Patient Access

Accessibility
- Data must be aggregated from multiple providers
- No standardized electronic format to create user-friendly integrated data set

Timeliness
- Long time period to provide copies impedes use of data for time-sensitive medical care
- No simple mechanism for refreshing/updating data

Cost
- Fees can become substantial for large record sets
- New fees payable for each updated data request
Evolution of Regulatory Framework to Promote Patient Access to Data

**Initial HIPAA Rule**
Access to records of single covered entity
Each covered entity determines format of records (including paper or electronic form)

**Amended HIPAA Rule**
Covered entity obligated to provide data in electronic form at patient’s request
Patient may direct disclosure to third party custodian

**Proposed CMS Rule**
Health plans obligated to share data with app developers through APIs
Standardized format mandated by CMS and ONC

Key Data Sharing Issues Driving Regulatory Change | Manatt, Phelps & Phillips, LLP
Potential Benefits and Risks of Reliance on Proposed App Model

**Potential Benefits**

- Opportunity for patients to aggregate data from multiple sources in single format to get alerts and see complete picture of their health
- Improves capacity for timely patient and provider decision-making
- May minimize duplication of services and reduce health care costs

**Potential Risks**

- Once data in apps they are not protected by HIPAA; FTC Act may not provide sufficient safeguards
- Patient consent may be inadequate in app environment
- Who vets apps for integrity and safety—what is the app business model?
- Mobile phone security becomes critical
Reasons for Data Blocking Within Health Care System

**IT Vendors**
- Promote acquisition of vendor’s EHR through closed community of data sharers
- Encourage use of vendor’s preferred ancillary products and services
- Direct resources toward functionality that improves marketplace position (charge high fees for other functionality)

**Providers**
- Reduce patient referrals outside of provider’s system
- Prevent cost or quality of care analyses that can be used for competitive purposes
- Preclude use of data for research by competing academic institutions
- Avoid fallout from data breaches at other entities
ONC Information Blocking Rule: Examples of Interpretive Challenges

- How will sensitive data subject to heightened legal restrictions be filtered?
- How will it be determined when a vendor or provider charges “excessive fees” for interfaces?
- What standards will organizations use to determine if a non-covered entity’s privacy policies are adequate?
- When does the refusal to share information promote data security?
- When are licensing terms for interoperability elements nondiscriminatory?
Evolution of Marketplace Toward Greater Data Sharing

- Siloed maintenance of records by individual covered entities
- One-to-one electronic exchanges with reduced information blocking
- Community-wide exchange through regional health information organizations?
## HIPAA Covered Entities vs. Health App Developers

<table>
<thead>
<tr>
<th>Laws regulating use and disclosure of health information</th>
<th>Covered Entities</th>
<th>App Developers</th>
</tr>
</thead>
<tbody>
<tr>
<td>- HIPAA—patient authorization required unless exception applies (TPO)</td>
<td>- State and federal laws governing sensitive data</td>
<td>- FTC Act—liability for “deceptive” and “unfair” practices</td>
</tr>
<tr>
<td>- FTC Act (see app developers)</td>
<td></td>
<td>- CCPA (et al?)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role of data in business model</th>
<th>Covered Entities</th>
<th>App Developers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient data used primarily to deliver the service the patient is requesting; commercialization is secondary</td>
<td>User data commonly commercialized for purposes unrelated to the service obtained through the app—this is central to business model</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Core tendencies</th>
<th>Covered Entities</th>
<th>App Developers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and restricted use</td>
<td>Transparency and sharing</td>
<td></td>
</tr>
</tbody>
</table>

Key Data Sharing Issues Driving Regulatory Change | Manatt, Phelps & Phillips, LLP
When Is an App Developer a Business Associate?

- Is app offered to consumers “on behalf of” health care provider or health plan?

- Factors likely to include:
  - How app is branded
  - Whether consumer accesses app through covered entity or separate channel
  - Whether app (or enhanced version) is available only through covered entity (i.e., only to provider’s patients or plan’s members)
  - How data flows between covered entity and app developer
  - Whether app developer provides any related services to covered entity
Challenges When Covered Entities and App Developers Interact

**Guidance for Industry**
- Can regulatory guidance provide greater certainty on when an app developer is a business associate?
- Can guidance keep up with rapid change in technology and marketplace?

**Clarity for Patients**
- How can it be made clearer to patients/users when their data is protected by HIPAA and when it is not?
- Do benefits of data sharing outweigh a certain amount of consumer confusion?

**Regulatory Limits on Certain Behavior**
- Is user consent ever inadequate as protective measure?
- Should government restrict certain data uses even with user consent?
Robert Belfort
Manatt, Phelps & Phillips, LLP
7 Times Square
New York, NY 10036
(212) 830-7270
rbelfort@manatt.com
Discussion

• What pending regulations will most impact eHI’s membership?
Steve Kastin, MD

Senior Executive Advisor and Chief Medical Information Officer (CMIO), Booz Allen Hamilton
Discussion

Discussion

- Where do privacy regulations contradict each other?
Discussion

- Where is more guidance on regs needed?
Discussion

- Where can eHI help educate congressional leaders and regulators on industry needs and concerns?
Discussion

- Are there key terms or regulations that are unclear to providers, consumers, others?
Discussion

- Think about the presentation from Maria this morning, what are your greatest concerns about HIPAA 2.0?
Next Steps