Background / conflicts

- 10+ years in health care technology and services, including:
  - Population health analytics
  - Ambulatory EHR vendor
  - Claims clearinghouse

- 2018 – 2019 RWJF Health Policy Fellow
  - Senate HELP Committee staff

- Co-author (with Lisa Bari):
  - “Rethinking Patient Data Privacy In The Era Of Digital Health” (Health Affairs, December 2019)

- No current conflicts
Agenda

1. What is happening
2. Why this is happening
3. Where we go from here
Traditional providers sharing data – at scale – with tech firms with checkered privacy record

Hospitals Give Tech Giants Access to Detailed Medical Records

Deals with Microsoft, IBM and Google reveal the power medical providers have in deciding how patients’ sensitive health data is shared.

Hospitals have granted Microsoft Corp., IBM Machines Corp. and Amazon.com Inc. patient information under deals to crunch data.

Google’s ‘Project Nightingale’ Gathers Personal Health Data on Millions of Americans

Search giant is amassing health records from Ascension facilities in 21 states; patients not yet informed.

Google is engaged with one of the U.S.’s largest health-care systems on a project to collect and crunch the detailed personal-health information of millions of people across 21 states.

The initiative, code-named “Project Nightingale,” appears to be the biggest effort yet by a Silicon Valley giant to gain a toehold in the

“The data belongs to whoever has it.”

-- Lisa Bari
Consumer health tools using patient health data to build enterprise businesses

Is your pregnancy app sharing your intimate data with your boss?

As apps to help moms monitor their health proliferate, employers and insurers pay to keep tabs on the vast and valuable data

By Drew Harwell

April 10, 2015

Like millions of women, Diana Diller was a devoted user of the pregnancy-tracking app Ovia, logging in every night to record new details on a screen asking about her bodily functions, sex drive, medications and mood. When she gave birth last spring, she used the app to chart her baby’s first online medical data — including her name, her location and whether there had been any complications — before leaving the hospital’s recovery room.

But someone else was regularly checking in, too: her employer, which paid to gain access to the intimate details of its workers’ personal lives, from their trying-to-conceive months to early motherhood. Diller’s bosses could look up aggregate data on how many workers using Ovia’s apps had faced high-risk pregnancies or gave birth prematurely... and how soon the new moms planned to return to work.”
EHR vendors blur the lines between patient- and provider-controlled data to build advertising businesses

How private is your health data on “patient portal” websites used by hospitals and doctors’ offices?

It’s not as private as you might hope, despite a federal law known as HIPAA, short for the Health Insurance Portability and Accountability Act.

A reader from Silver Spring, Md., who asked me not to use her name, emailed me after reading the privacy policy in an external website used by her doctors at George Washington University Medical Faculty Associates. The patient portal FollowMyHealth.com reserves rights to use “personal health record” data for “marketing and advertising purposes, including sending you marketing and advertising communications whether on our behalf or on behalf of marketing partners.”

When I contacted Follow My Health’s corporate parent Allscripts, it painted a narrower picture of its practices — and claimed the site wasn’t limited by HIPAA.

Tom Lynch, the company’s director of marketing communications, said the site is “not disclosing identifiable patient data to third parties for any marketing purpose” — even though its privacy policy specifically reserves the right to “release” personal health data for marketing and advertising. (That policy was updated in August.)

“…using ‘information about patients to alert them to certain goods and services…””
Recap: For good or ill, more patient data is flowing across organizational & regulatory boundaries

Traditional **healthcare providers** (aka HIPAA covered entities) are pursuing business opportunities which rely on patient data, often in partnership with non-traditional actors

- Generally in aggregated, de-identified form

**Digital health services** (not covered entities) are collecting data directly from consumers, but then using it to build new revenue streams from employers, insurers, drugmakers etc

**Electronic health records** (aka HIPAA business associates) are working to shift health data from a provider-controlled to a patient-directed regulatory regime, to open up new business opportunities
“In the future, everyone will want to be anonymous for fifteen minutes.” Banksy
Agenda

1. What is happening

2. Why this is happening

3. Where we go from here
Digital health brings opportunities for research and care delivery, but with acute privacy risks

- Novel research methods / opportunities
- Improved care delivery
- Non-clinical businesses (e.g. advertising)
- Patient / consumer privacy and discrimination concerns

Commercially-oriented healthcare system

- (Rapid) growth in available data
- Expanded patient engagement / access
- New ‘providers’ / care delivery models
- Outdated regulatory framework
HIPAA’s data protections revolve around entities, not the data itself

**HIPAA’s conceptual structure (simplified!)**

1. **Establish a list of “Covered entities”**
   - Providers (hospitals, physician practices, etc)
   - Health plans (insurers and ERISA plans)
   - Clearinghouses

2. **Define a category of data**
   - Individually identifiable health information (IIHI)
   - “information...that relates to the individual’s past, present or future physical or mental health...the provision of health care to the individual, or... payment for the provision of health care to the individual”

3. **Assign data protection obligations to those entities**
   - Conditions for sharing or disclosure (“payment, treatment or operations,” “minimum necessary” etc)
   - Patient access rights (often ignored)
   - Breach notification & security rules
Siloed HIPAA framework opens door to regulatory arbitrage and the erosion of public trust

Not an exhaustive list

- **Shift the source** → **Change the rules**
  - Given HIPAA’s entity orientation, data collected from a patient (or derived from patient-sourced data) lacks equivalent privacy and security protections

- **Shift “control”** → **Change the rules**
  - Provider-sourced clinical data shifted to patient’s control can free the data (and the entity that holds the data) from HIPAA protections and access rights

- **“De-identify”** → **Change the rules**
  - De-identified data is no longer deemed “individually identifiable,” hence is not “protected” and hence no longer subject to the same protections and consent requirements

Money in politics healthcare is like water on pavement...
...It finds every crack and crevice.
Some of these exploitable “loopholes” also serve systemic goals with clear social benefit

Example:

- Patient control and consent
- Research flexibility and efficiency
Meanwhile, some providers lean on “privacy” to serve business objectives at variance with patient interests.

Example:

*Provider / incumbent control*

*Patient access & competition*
Agenda

1. What is happening

2. Why this is happening

3. Where we go from here
“...Adapt and extend the familiar HIPAA framework, and some of the fiduciary principles embedded in that framework, for a new era of digital-first health care.”
# Contrast with more recent privacy law – GDPR & CCPA – highlights HIPAA gaps

<table>
<thead>
<tr>
<th></th>
<th>HIPAA (current)</th>
<th>GDPR</th>
<th>Adapted / extended HIPAA (proposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health data in scope</strong></td>
<td>Individually identifiable health information (IIHI), relating to individual health (physical or mental), provision of care or payment for provision of care, <em>when that IIHI is held or transmitted by a covered entity or its business associate</em></td>
<td>“Personal data” which includes direct or indirect identifiers and “expresses the physical, physiological, genetic, mental, commercial, cultural or social identity” individuals. Health data is a special category with heightened protection.</td>
<td>IIHI relating to an individual health (physical or mental), provision of care, or payment for provision of care, regardless of who collects, holds, processes or transmits that data</td>
</tr>
<tr>
<td><strong>Regulated entities</strong></td>
<td><strong>Covered entities (CEs)</strong> – Health plans, health care providers and health care clearinghouses</td>
<td><strong>Controller</strong> – Any person or organization which determines the purposes or means of processing personal data</td>
<td><strong>Custodian</strong> – Any person or organization collecting or holding IIHI, or controlling the processing thereof</td>
</tr>
<tr>
<td></td>
<td><strong>Business associates</strong> – person or organization performing functions on behalf of (or providing services to) a CE</td>
<td><strong>Processor</strong> – person or organization processing data on behalf of controller</td>
<td><strong>Processor</strong> – person or organization processing data on behalf of custodian</td>
</tr>
<tr>
<td><strong>Permitted uses of personal health data</strong></td>
<td>Health care treatment, payment and operations</td>
<td>Treatment, public health, research, judicial proceedings, substantial public interest, by informed consent, or when processing is in the “vital interests” of person unable to consent</td>
<td>Health care treatment, payment and operations, regardless of the entities involved in those activities, when appropriately disclosed to the individual. All other uses require consent.</td>
</tr>
<tr>
<td><strong>Security standards</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Breach notification requirements</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Individual right to:</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✖️</td>
</tr>
<tr>
<td>Access</td>
<td>Amend</td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

Five key steps to modernize HIPAA for the era of digital health

1. Define *individually-identifiable health information (IIHI)* as an inherently protected class of data, regardless of who holds or processes the data.

2. Create new definitions of IIHI “custodians” and “processors” – analogous to (but broader than) HIPAA’s covered entities and business associates.

3. Establish individuals’ right to access, amend and delete IIHI, and to consent to or decline participation in aggregated data sets.


5. Specific parameters for consumer-friendly and revocable consent, for any use or disclosure beyond narrow permitted uses.
Discussion