Welcome
Welcoming Remarks
Commissioner Brill
Health Data Flows

Latanya Sweeney
Chief Technologist, FTC
Transparency Establishes Trust
Disclaimer

The views and opinions in this presentation represent my own and are not necessarily those of the U.S. Federal Trade Commission. These views are for the benefit of public discourse and public education, and are not necessarily an opinion regarding any position I may take on related issues decided by the FTC.
Transparency Establishes Trust
Establishes Distrust
You, the Patient

Physician, Hospital

thedatamap.org
33 States Sell or Share Personal Health Data

Only 3 States Use HIPAA Standards

thedatamap.org/states.html
<table>
<thead>
<tr>
<th>Purchaser</th>
<th>States that Sold Purchaser Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truven Health Analytics</td>
<td>AZ, CA, FL, IL, MD, MA, NJ, NY, PA, TN, WA</td>
</tr>
<tr>
<td>Optuminsight (Ingenix)</td>
<td>CA, FL, IL, MD, MA, NJ, NY, PA, TX, WA</td>
</tr>
<tr>
<td>Milliman</td>
<td>AZ, CA, FL, IL, MD, MA, NY, TN, TX, WA</td>
</tr>
<tr>
<td>WebMD Health</td>
<td>AZ, CA, IL, MD, NJ, NY, PA, TN, WA</td>
</tr>
<tr>
<td>IMS Health (SDI Health and Verispan)</td>
<td>AZ, FL, IL, MD, NJ, NY, PA, TN, WA</td>
</tr>
<tr>
<td>Intellimed International</td>
<td>AZ, CA, FL, MD, NY, TX, WA</td>
</tr>
<tr>
<td>Service Employees International (SEIU)</td>
<td>CA, FL, MD, MA, PA, TN, WA</td>
</tr>
<tr>
<td>DataBay Resources</td>
<td>CA, FL, MA, NY, PA, WA</td>
</tr>
</tbody>
</table>
Record: 505825338
Hospital: 162: Sacred Heart Medical Center in Providence
Admit Type: 1: Emergency
Type of Stay: 1: Inpatient
Length of Stay: 6 days
Discharge Date: Oct-2011
Discharge Status: 6: Disch/Trfn to home under the care of an health service organization
Charges: $71708.47
Payers: 1: Medicare
   6: Commercial insurance
   625: Other government sponsored patients
Emergency Codes: E8162: motor vehicle traffic accident due to loss of control; loss control mv-mocycl
Diagnosis Codes: 80843: closed fracture of other specified part of pelvis
   51851: pulmonary insufficiency following trauma & surgery

86500: injury to spleen without mention of open wound into cavity
80705: closed fracture of rib(s); fracture five ribs-close
5849: acute renal failure; unspecified
8052: closed fracture of dorsal [thoracic] vertebra without mention of spinal cord injury
2761: hyposmolality &/or hyponatremia
78057: tachycardia
2851: acute posthemorrhagic anemia

Age in Years: 60
Age in Months: 725
Gender: Male
ZIP: 98851
State Reside: WA
Race/Ethnicity: White, Non-Hispanic
MAN, 60, THROWN FROM MOTORCYCLE
A 60-year-old Soap Lake man was hospitalized Saturday afternoon after he was thrown from his motorcycle. Ronald Jameson was riding his 2003 Harley-Davidson north on Highway 25, when he failed to negotiate a curve to the left. His motorcycle became airborne before landing in a wooded area. Jameson was thrown from the bike; he was wearing a helmet during the 12:24 p.m. incident. He was taken to Sacred Heart Hospital. The police cited speed as the cause of the crash.
[News Review 10/18/2011]
Washington State Health Database
43% news stories re-identified

News stories have same information that others know. Employers, Creditors, Family, Friends and Neighbors
Transparency Establishes Trust
A Snapshot of Data Sharing by Select Health and Fitness Apps

FTC Staff’s Preliminary Observations
Examined 43 free and paid health and fitness apps
  o Wearables not included

Traffic analysis and privacy policy review

Findings:
  o 26% of the free apps and 40% of the paid apps did not have a privacy policy
  o 39% of the free apps and 30% of the paid apps sent data to someone not disclosed by the developer either in-app or in any privacy policy they found
  o 13% of the free apps and 10% of the paid apps encrypted all data connections between the app and the developer’s website.

Conclusion:
“Our research brought us to the conclusion that, from a privacy perspective, mobile health and fitness applications are not particularly safe when it comes to protecting user privacy.”

Evidon
A Healthy Data Set- September 2013

• Tested 20 health and fitness apps
• Found the presence of 70 third parties

• “These companies are typically advertising and analytics companies, who attempt to better match advertisements to users who will buy; and who work to help app developers increase functionality and usability, respectively.”

Source: http://www.evidon.com/blog/healthy-data-set
WHO and WHAT?
Reconceptualizing the Evidon Study
Health & Fitness App Snapshot

Methodology

- Twelve apps and two wearables
- App traffic analysis
- Mapped the data sets
Health & Fitness App Snapshot

Limitations

• One device
• Only Free Apps
• Front-end testing only
• Did not review privacy policies
**App Example**

One app transmitted information to 18 different 3rd parties. Information included:

*Device Information*
*Device & 3rd Party Identifiers*
*Consumer Specific Identifiers*
*Workout/Route Information*
*Diet Information*
3rd Party Example
Four apps transmitted the following information to the same 3rd party. Information included:

* Identifiers common between the apps
* Device information
* Gender
* Workout Information
* App Category
Observation #1
18 third-parties received Device Specific Identifiers such as:

*Device ID
*MAC address
*IMEI
Observation #2
14 third-parties received Consumer Specific Identifiers such as:

*Username
*Name
*Email Address
Observation #3
22 third-parties received additional information about consumers such as:

* Exercise Information
* Meal/Diet Information
* Medical/Symptom Search Information
* Zip code
* Geolocation
* Gender
Summary of Observations

• Health and fitness apps collect and transmit to third parties sensitive information about our bodies and our habits.

• The 12 apps tested transmitted information to 76 different third-parties. This information included:
  
  - Device Information;
  
  - Consumer specific identifiers;
  
  - Unique device IDs capable of allowing 3rd parties to track users’ devices across apps;
  
  - Unique 3rd party IDs capable of allowing 3rd parties to track users’ devices across apps; and
  
  - Consumer information such as exercise routine, dietary habits, and symptom searches.

• There are significant privacy implications where health routines, dietary habits, and symptom searches are capable of being aggregated using identifiers unique to that consumer.
Panel Discussion

- **Christopher R. Burrow**, M.D., EVP Medical Affairs, Humetrix
- **Joseph Lorenzo Hall**, Chief Technologist, Center for Democracy & Technology
- **Sally Okun**, RN, MMHS, Vice President of Advocacy, Policy & Patient Safety, PatientsLikeMe
- **Heather Patterson**, Postdoctoral Research Fellow, New York University
- **Joy Pritts**, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology, Department of Health & Human Services
Mobile Anytime/Anywhere Access to Personal Health Records
Access to e-Health Records is a Right Ensured by HIPAA

Important tools like Electronic Health Records (EHRs) and Personal Health Records (PHRs) will make it easier, safer, and faster for you to get access to your health information and stay engaged.

Message from Leon Rodriguez, Director, Office for Civil Rights

Many consumers want to play a more active role in their health care. The right to see and get a copy of your medical records

Children’s doctor visits. Health information is critical to all patients so that they can track their progress through wellness programs, monitor chronic conditions, communicate with their treatment teams, and adhere to their important treatment plans. Important tools like Electronic Health Records (EHRs) and Personal Health Records (PHRs) will make it easier, safer, and faster for you to get access to your health information and stay engaged. These tools help you become a true partner in your health care and wellness.

I also know that, all too often, consumers face barriers to getting their health information – and the first barrier is that many do not know their rights. You should know you have the right to:

- Ask to see and get a copy of your health records from most doctors, hospitals, and other health care providers such as pharmacies and nursing homes, as well as from your health plan;
- Get either a paper or, if records are kept electronically, an electronic copy of your records; and
- Have your provider or health plan send a copy of your records to someone else.

To make sure you know your rights and are able to assert those rights, my office has developed videos, pamphlets, answers to questions, and other guidance to help you understand your rights under HIPAA. To find these tools, go to our website, www.hhs.gov/ocr, and:
iBlueButton Display & Aggregation of TRICARE, VA, Medicare Blue Button and EMR Records (Epic, Cerner, Allscripts etc...)
Patient Generated Data
Health Care Proxy and Prior Discharge Summaries
Imported into iBlueButton
Consumer-Controlled Mobile Health Record Access & Exchange

EHRs from diverse sources (e.g. hospitals, payers, HCP groups)

Mobile-to-Mobile Exchange of Blue Button® and other records at the Point of Care

Patient to Physician

Provider’s iPad App

Patient’s iOS & Android App

Physician back to Patient

huMETRIX®
iBlueButton for Medicare Beneficiaries: Three Years of Medical History in Patients’ Hands for their Safety

From Blue Button…

From a 300 page Blue Button ASCII text claims record to…

…a mobile longitudinal health record available at every Point of Care
Providers Transmit Records to their Patients’ Unique iBlueButton Address using the Secure Federal Direct Transport Standard

Data Holder

susan.jones@direct.ibluebutton.com

securely sends health records when ever her record changes

Provider

App

Some PHR

Provider Interface - Transmit Using Direct

(1) Provider accesses patient record

(2a) Provider clicks “Share” and verifies patient authorization

(2b) Provider clicks “Add Direct Address” and verifies patient authorization

(3a) Provider enters Direct Address and selects frequency

(3b) Provider enters Direct Address to automatically send updates to

iBlueButton App generates a Direct Address for each Profile
iBlueButton: Display of Medicare, EMR, VA and TRICARE records with Real Time Aggregated View
Patient Generated Data
Medication and Condition Annotations and Privacy Settings

Medications
- Paroxetine Hydrochloride
- Zolpidem Tartrate
- Atenolol 50Mg
- Furosemide 40Mg Tab
- Benazepril Hcl 40Mg

Are you currently taking this?
Experiencing any side effects?
Keep this entry private?

- nausea
- dizziness

Conditions
- Major depression in remission
  - Currently experiencing this?
  - Condition reported in error?
  - Keep this entry private?
Details: Major depression in remission (disorder)

- Headache
- Hypertension NOS
What are Humetrix's PHR data practices for iBlueButton?

Use this page to understand how Humetrix and our service providers release and secure your PHR Data.

### Release

<table>
<thead>
<tr>
<th>Do we release your PHR Data for these purposes?</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do we require Limiting Agreements that restrict what third parties can do with your Personal Data?</td>
<td>N/A</td>
</tr>
<tr>
<td>Do we stop releasing your Personal Data if you close or transfer your PHR?</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>We release...</th>
<th>Personal Data</th>
<th>Statistical Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>For marketing and advertising</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>For medical and pharmaceutical research</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>For reporting about our company and our customer activity</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>For your insurer and employer</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>For developing software applications</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Secure

We have security measures that are reasonable and appropriate to protect personal information, such as PHR Data, in any form, from unauthorized access, disclosure, or use.

<table>
<thead>
<tr>
<th>Do we store PHR Data in the U.S. only?</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do we keep PHR Data activity logs for your review?</td>
<td>No</td>
</tr>
</tbody>
</table>
Panel Discussion

• **Christopher R. Burrow**, M.D., EVP Medical Affairs, Humetrix

• **Joseph Lorenzo Hall**, Chief Technologist, Center for Democracy & Technology

• **Sally Okun**, RN, MMHS, Vice President of Advocacy, Policy & Patient Safety, PatientsLikeMe

• **Heather Patterson**, Postdoctoral Research Fellow, New York University

• **Joy Pritts**, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology, Department of Health & Human Services