The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly?

Vishakha Kumari, M.S. student, Human-Computer Interaction
Sara Anne Hook, M.B.A., J.D., Professor of Informatics/Human-Centered Computing

Introduction

- One in every ten Americans uses a wearable device
- Monitor and record physical activity and sensitive health information
- Perceive and record information continuously- Amount of information increasing

Advantages of Wearable Health Devices

- Transforming health care industry
- Insights to health with ease
- Bringing health revolution
- Research/predict the future of human health care needs
- Plan for the health care resources (personnel, facilities, resources) that will be needed in the future

Concerns with Wearable Health Devices

- Storage and re-use of protected health information
  - Privacy
  - Security
  - Discoverability as part of litigation, an investigation, an audit, etc.
- Still an evolving field with no specific state or federal laws expansive enough to protect the health data collected by these devices

Privacy and Security Issues with Wearable Health Devices

- Identity theft, profiling, stalking, extortion, discrimination
- Health information is considered more profitable than SSNs in black market
- Bad credit, inaccurate health records, higher premiums and loss of insurance coverage are a few examples of problems which may arise

Discoverability of Data from Wearable Health Devices

- Part of overall Internet of Things (IoT)
- Promise a whole new era of forensic science
- Data from wearable health devices used as “witness” in court cases – civil and criminal

Glimpses of Wearable Devices in the Justice System

- In March 2015, a 44-year-old woman in East Lampeter Township, Pennsylvania, lied about being sexually assaulted. Data from her fitness device showed that she was awake and walking around when she said that the attack happened.
- In 2014, Canadian law firm introduced Fitbit data to show that its client was suffering from injuries sustained in an automobile accident. Aggregated data showing her activity measurements was compared to other wearers' data to prove the plaintiff was less active than women her age and her profession.

Glimpses of Wearable Devices in the Justice System

- Richard Dabate, 40, was charged with felony murder, tampering with physical evidence and making false statements following his wife Connie's December 2015 death at their home in Ellington, Tolland County.

State police used an analysis of the home's "alarm system, computers, cellphones, social media postings and Connie Dabate's Fitbit to create a timeline that contradicted Richard Dabate's statements to police," proving him guilty of his wife's murder.

Discoverability Concerns of Data from Wearable Health Devices

- Must meet the tests for admissibility as outlined in the Federal Rules of Evidence, Federal Rules of Civil Procedure (as amended on December 1, 2015) and corresponding state court rules:
  - Reliability
  - Authenticity
  - Not prejudicial
  - Probative value
  - Relevant

What U.S Federal Legislation May Apply to Wearable Health Devices?

- Health Care Portability and Accountability Act (HIPAA) and the HITECH Act
- Federal Trade Commission (FTC)
- Food and Drug Administration (FDA)

U.S. Federal Laws - HIPAA

- HIPAA "provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information."

- Wearable health devices may not be covered under HIPAA because -
  - Only Health Care Providers, Health Care Clearinghouses and Health Plans are required to comply to HIPAA regulations
  - Health information from wearable health devices is not Protected Health Information(PHI)

U.S. Federal Laws - FTC

- Federal Trade Commission (FTC)- Prohibits unfair and deceptive trade practices
- The FTC has, through its enforcement, focused on privacy and in ensuring that companies comply with their stated privacy policies
- Attempts to protect consumer data in general and not specially targeted towards setting guidelines for protecting data from wearable devices

U.S. Federal Laws - FDA

- The Food and Drug Administration (FDA) is a U.S agency in charge of protecting and promoting public health through the control and supervision of regulated medical devices
- Fitness trackers likely would be placed into the category of “low risk general wellness” devices and thus do not require FDA oversight

U.S. State Laws - Indiana

- Indiana Code 24-4.9 covers the disclosure of a security breach, which includes definitions for terms such as breach of the security of data, database owner, encrypted data, “person” and personal information, requirements for disclosure and notification of a breach, the duties of a database owner, the methods of disclosure, penalties for disclosure and the actions that can be taken by the Attorney General
- Indiana Code 4-1-6 features its Fair Information Practices and Privacy of Personal Information
- Finally, Indiana Code 4-6-14 is devoted to the protection of health records and identifying information

U.S. State Laws - Massachusetts

- The law in Massachusetts includes regulations on the protection of personal information
    - Its definitions for “persons” and “personal information” are expansive
    - Its Standards for the Protection of Personal Information of Residents of the Commonwealth cover purpose and scope, definitions, duty to protect and standards for protecting personal information
- Interestingly, this statute includes computer system security requirements, making it particularly compelling as guidance for implementing a comprehensive security program

U.S. State Laws - Washington

- The Uniform Health Care Information Act, enacted in 1991, is Washington State’s primary health data protection legislation
- It also focuses on the rights to access health care information
- Washington State’s current health information protection laws provide protection similar to HIPAA for traditional health care information and the state constitution is considered one of “a handful of state constitutions that explicitly protects privacy”

Recommended Next Steps

- Design Recommendations-
  - Choice to opt out of any terms and conditions
  - Visibility of relevant privacy information
  - Private default settings

Recommended Next Steps

- Law Amendments-
  - Specific laws targeted towards the “wearables” industry
  - Expand the definitions of “covered entities,” “individually identifiable health information” and “third parties”
  - The Federal Trade Commission (FTC) can be more active in oversight regarding the privacy and security of personal information

Recommended Next Steps

- Other options – for consumers
  - Read policies carefully and understand the risks.
  - More awareness
  - User education
  - Option to check and change information sharing settings
  - Private default settings

Conclusion : Data from Wearable Health Devices: Fitness or Folly?

- Public unaware of security and privacy concerns
  - Will this change after some high-profile cases or incidents?
- Experts calling for new regulations
- Proposed amendments to the Federal Rules of Evidence to address concerns with digital evidence

Any Questions?

Thank you for attending this session of HCI International 2017!