Drug and Device Privacy and Cybersecurity Considerations

Seth Carmody, Cybersecurity Program Manager, CDRH, FDA
Kimberly J. Gold, Partner, Reed Smith LLP
Tara Sklar, Professor of Health Law, University of Arizona

Drug and Device Privacy and Cybersecurity Considerations

Kimberly J. Gold

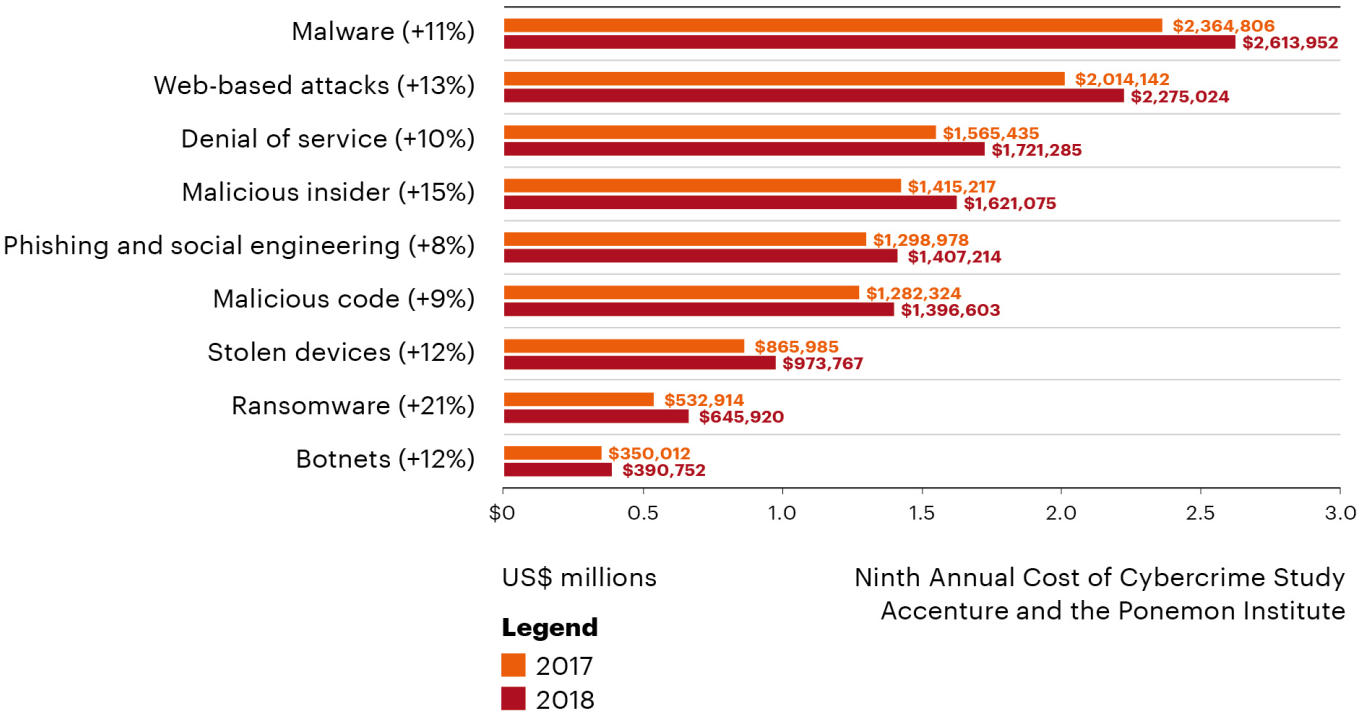
Partner, Reed Smith LLP

“Personal data is the oil of the 21st century, a resource worth billions to those who can most effectively extract and refine it.”

Source: NYTimes, Dec. 18, 2018

Cybersecurity Threats

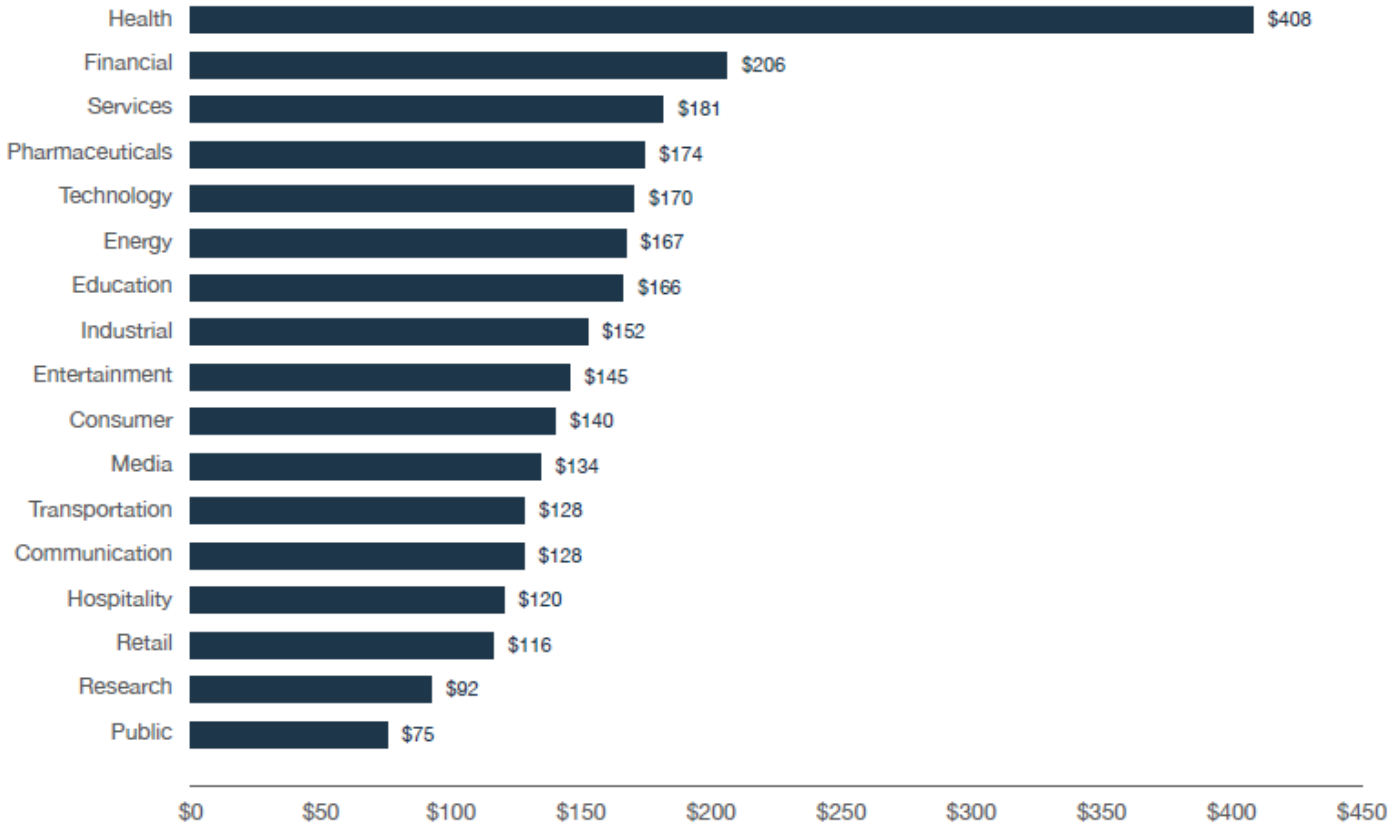
Average annual cost of cybercrime by type of attack (2018 total = US$13.0 million)



Ninth Annual Cost of Cybercrime Study
Accenture and the Ponemon Institute

Figure 7. Per capita cost by industry sector

Measured in US$



*Source: IBM Security/Ponemon Institute 2018 Cost of a Data Breach Study

Sources of Cybersecurity Guidance

- FDA Premarket and Postmarket Guidance
- NIST Cybersecurity Framework
  - Identify, protect, detect, respond, recover
- HHS/HIPAA Security Rule
  - Recently released Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- FTC - Start with Security: A Guide for Business
- DOJ guidance
- State AGs
- SEC guidance on public company cybersecurity disclosures
- Certifications/standard-setting bodies (e.g., ISO)

Legal Risk Environment

- Federal Privacy Laws and Regulations
- State Privacy Legal Landscape
- International Requirements (GDPR)
- Cybersecurity and Privacy Guidance
- PCI DSS
- Contractual Obligations
- Litigation/Class Actions (Spokeo and Target)

U.S. Federal Law Overview

- Federal Trade Commission (FTC) Act (Section 5)
- Children's Online Privacy Protection Act (COPPA)
- Electronic Communications Privacy Act (ECPA)
- Telephone Consumer Protection Act (TCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
- Health Insurance Portability and Accountability Act (HIPAA)
- Privacy Act (applicable to US Government databases)
- Gramm-Leach-Bliley Act (GLBA)
- Computer Fraud and Abuse Act (CFAA)
- Fair Credit Reporting Act (FCRA)
- Communications Act

State Privacy Legal Landscape

- Attorneys general / Consumer protection
- State data breach notification laws
- Biometric laws (e.g., Illinois Biometric Info. Privacy Act)
- State general privacy, data security, secure disposal laws (e.g., CCPA)
- Private litigants
  - Class actions in the wake of a data breach
  - Marketing privacy class actions

State Breach Notification Laws

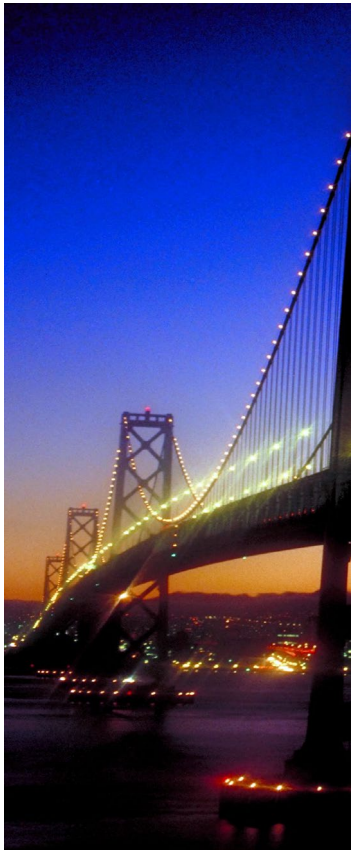
- All 50 U.S. states, and the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted breach notification laws that require businesses to notify consumers if their personal information is compromised
- Despite the variation in U.S. states' data breach laws, they cover similar types of information and all states have a defined list of covered information
- Reporting timing requirements vary
- Potential for high penalties
  - September 2018: Uber settled with state AGs for $148 million

State Biometric Laws

- Currently passed in Illinois, Texas, and Washington
  - Illinois Biometric Information Privacy Act (BIPA) is the most stringent and comprehensive
    - Requires companies collecting information such as facial, fingerprint and iris scans to obtain prior consent from consumers or employees, detailing how they'll use the data and how long the records will be kept
    - Allows private citizens to sue for violations
- More states are likely to follow suit
- Consumer litigation
  - Litigation against Six Flags Entertainment Corp. recently upheld by Illinois Supreme Court
    - Upheld consumers' right to sue companies for collecting data like fingerprint or iris scans without telling them how it will be used

California Consumer Privacy Act (CCPA)

- Sweeping new consumer-focused California privacy law
- Swift response to increasing public concern over general data protection and privacy
- Analogous to General Data Protection Regulation (GDPR)
- Affects businesses of all types, including retail companies, so long as such businesses have consumers in California
- Compliance efforts have begun, despite substantial legislative ambiguities



CCPA Applicability

- Any for-profit business doing business in California, that:
  - Has $25 million+ in revenue;
  - Annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the Personal Information of 50,000 or more Consumers' households or devices; or
  - Derives at least 50% of its annual revenues from selling Consumers' Personal Information.
- **Personal information:** includes information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
- **Consumer:** includes any "natural person who is a California resident . . . however identified, including by unique identifier."
- CCPA's applicability to the **employer-employee** relationship has been the subject of debate

What does the CCPA Require?

- Enhanced Privacy Notice Requirements
- Individual rights to request PI:
  - Access
  - Deletion – applies to company and vendors
- Choice and Consent for sale of PI:
  - Opt-out capabilities – “Do Not Sell My Personal Information” link on website
  - 800 number to opt-out

CCPA Exemptions

- Some, but not all, health and life sciences entities are subject to CCPA exemptions:
  1. Non-Profit Entities
  2. HIPAA Covered Entities and Business Associates
  3. Health Care Providers Subject to CMIA
  4. Certain Clinical Research

Future of Privacy Law in the U.S.

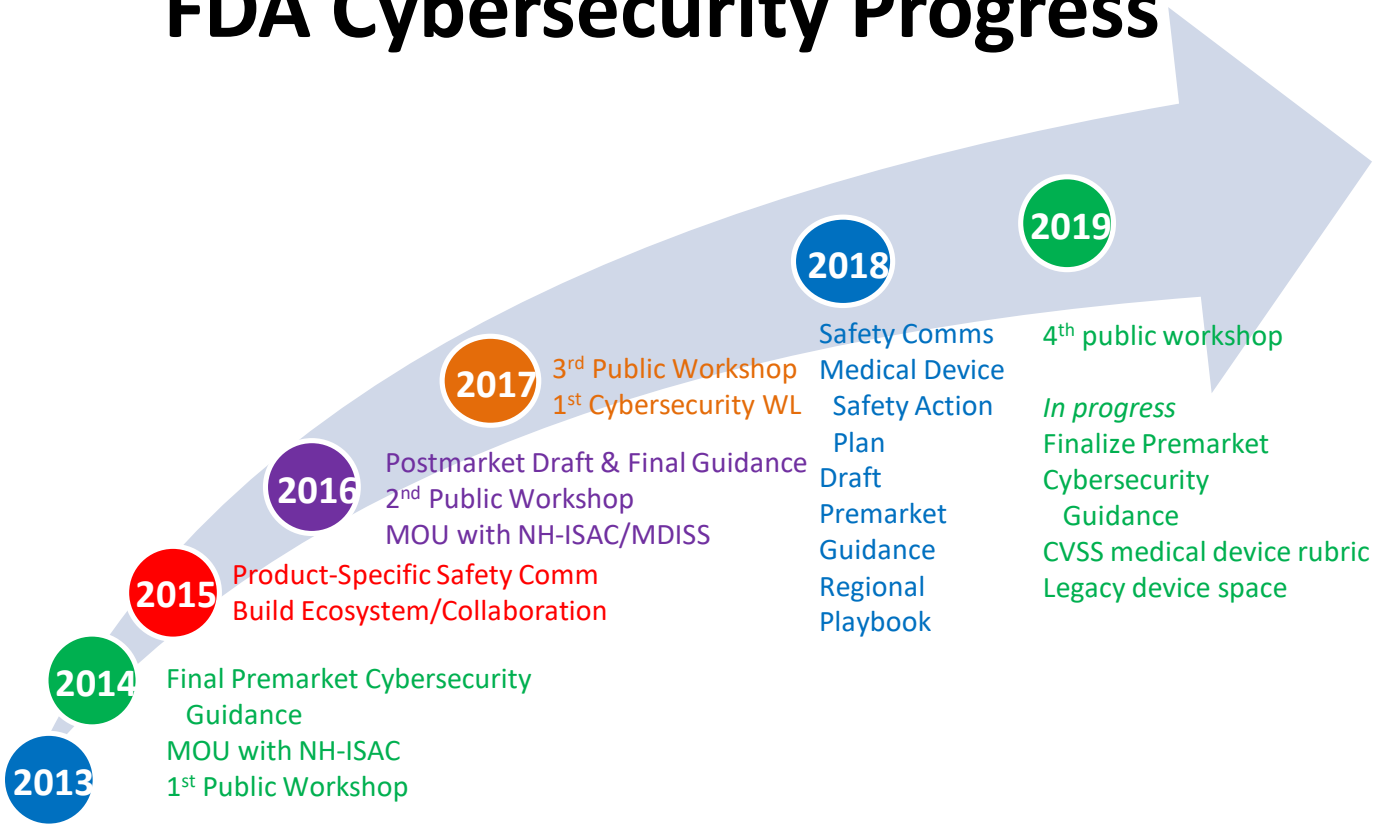
- Other states following California with proposed privacy laws
  - Vermont enacts first data broker legislation
  - Washington's proposed privacy act
  - New York's proposed consumer privacy/right to know law
  - Other states including Virginia, Vermont, Colorado, and New Jersey have all recently introduced related privacy regulations
- Potential federal law being considered
  - CCPA/GDPR like legislation a hot topic
  - American Data Dissemination Act
  - Social Media Privacy and Consumer Rights Act

DRUG AND DEVICE PRIVACY AND CYBERSECURITY CONSIDERATIONS

SETH D CARMODY, PHD, HCISPP
CDRH / FDA

MAY 3, 2019

FDA Cybersecurity Progress



2018 - 2019 Reflections

- Medical Device Safety Action Plan (April 2018)
- AAMI BI&T: The Evolving State of Medical Device Cybersecurity March/April 2018
- Perspective piece in American Heart Association Journal 'Circulation' (Sept 2018)
- Report on Advancing Coordinated Vulnerability Disclosure – MDIC publication (Oct 2018)
- FDA Commissioner's Statement (Oct 2018):
  - Strong commitment to efforts that bolster medical device cybersecurity
  - Regional Incident Preparedness & Response Playbook – MITRE publication (Oct 2018)
  - Execution of 3-way MOUs with H-ISAC for 2 newly stood up ISAOs for medical device vulnerability reporting (Oct 2018):
    - MedISAO
    - Sensato

2018 -2019 Reflections continued

- New FDA Draft Premarket Cybersecurity Guidance
- Execution of MOA with Department of Homeland Security
- HSCC Task Group 1B released Joint Security Plan Jan 28, 2019
- FDA convened Public Workshop, Jan 29-30, 2019

Looking Ahead 2019

- Complete CVSS clinical rubric & submit for MDDT qualification (MITRE-led WG)
- Further enhance public-private partnership collaborations to collectively address Imperative 2 of 2017 Task Force Report:
  - CYMSAB Pilot currently under development (with MITRE support)
  - Additional ISAOs in formation for device vulnerability info-sharing
  - Dedicated effort on defining and operationalizing Software Bill of Materials

Looking Ahead 2019 continued

- International Medical Device Regulators Forum (IMDRF) new medical device cybersecurity work item:
  - FDA and Health Canada co-leads
- Expand x-stakeholder participation in DefCon Biohacking Village Device Hacking Lab, with the following goals:
  - Increase medical device manufacturer (MDM) presence
  - Introduce to clinical community
  - Engage HDOs
- Leverage cross-agency / multi-stakeholder collaborative efforts:
  - NTIA (Dept of Commerce) Multi-stakeholder engagement on software component transparency includes representation on WGs from: HDOs, MDMs, device trade organizations and FDA
  - NCCoE (NIST/Dept of Commerce) working with industry to develop use cases for medical device security

Medical device cybersecurity is a shared responsibility

FDA contacts:

Suzanne.Schwartz@fda.hhs.gov
Seth.Carmody@fda.hhs.gov
Aftin.Ross@fda.hhs.gov

Or email the team:

CyberMed@fda.hhs.gov

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

Privacy Considerations in Clinical Research

Tara Sklar, JD, MPH
Professor of Health Law
University of Arizona College of Law

2019 FDLI Annual Conference

THE UNIVERSITY OF ARIZONA

Motivation

Global trend to increase individual rights over personal data

New opportunities and privacy risks with wearable technology

Escalation of the research participant role in clinical research

Data Privacy Regulation

General Data Protection Regulation (GDPR) 2016

CA Consumer Privacy Act (CCPA) 2018

Federal Data Privacy Legislation?

GDPR and CCPA

- Greater accountability to **secure and protect** consumer data and **enhance individual rights** over personal data
- Encourage transparency
- Report data breaches

Diverge and are silent…
Opt-in/Opt-out, Penalties, Research Exemption

Senate Judiciary Committee
GDPR & CCPA: Opt-ins, Consumer Control, and Impact on Competition & Innovation

- March 12, 2019 -- invited academics and industry members
- Bi-partisan support for federal action on privacy legislation

Dianne Feinstein (D-CA)

"*CCPA should serve as the floor for provisions in federal law*."

Jane Bambauer (Arizona Law)

"*We are interconnected. If I demand to close off information about myself, that doesn't just affect me, it affects the entire market*."

Industry perspective

"**Privacy isn't a slogan, it's vital to our business**."

Google Privacy Counsel, Will DeVries

"***Privacy is a human right, we need a GDPR for the world.***"

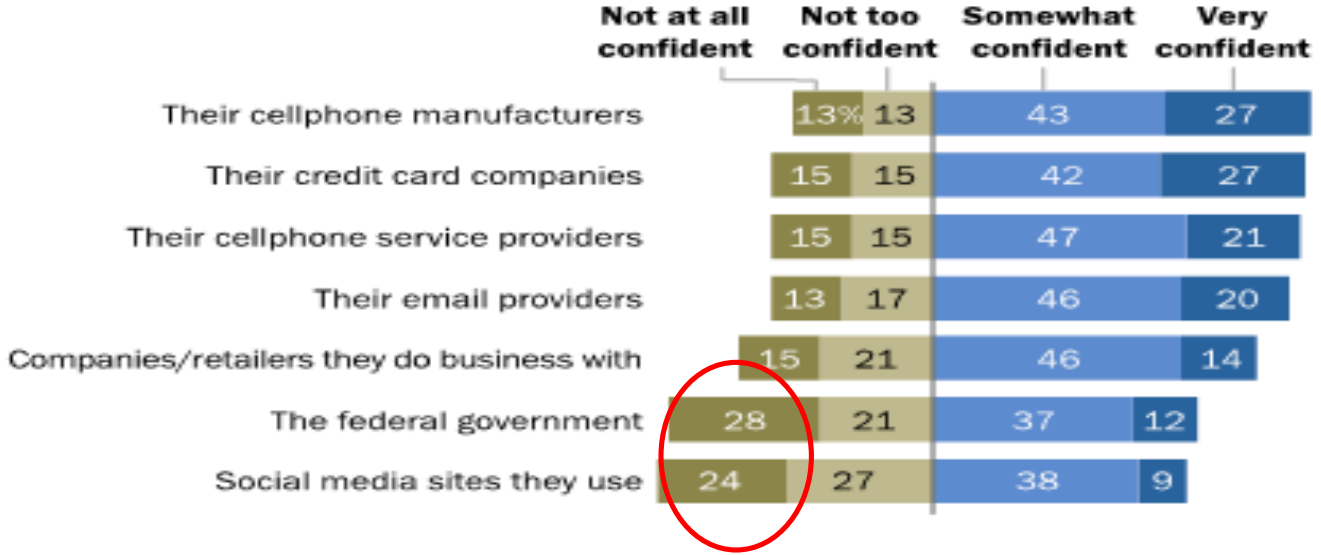
Microsoft CEO, Satya Nadella

"Legislation governing privacy will ***increasingly lag behind*** *the introduction of new technologies. This will exacerbate the problem of* ***inconsistent laws in different jurisdictions****."*

Biometric Institute

Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are ____ in the ability of the following institutions to protect their data



Note: Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies recalculated to exclude "does not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart.
Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Category	CCPA	GDPR
Rights granted	Grants consumers five rights: 1. Right to know **2. Right to delete** 3. Right to access **4. Right to opt-out** 5. Right to non-discrimination 6. Right to data portability	Grants data subjects eight rights: 1. Right to be informed 2. Right to access 3. Right to rectification **4. Right to erasure** **5. Right to restrict processing** 6. Right to data portability 7. Right to object 8. Rights in relation to automated individual decision making, profiling

Wearables in Clinical Trials

*"Ten years ago, there were a **million data points** in a big Phase III study.*

Today, we are talking about collecting
***millions of data points per research participant per day**."*

Vice President of Clinical Data at Veeva,
Richard Young


120 bpm
55:08 min
508
10,000 steps


KENZEN
ECHO H2 Smart Patch
Sport Performance Monitoring:
• Hydration
• Endurance
• Recovery

Friend or Foe? Your Wearable Devices Reveal Your Personal PIN

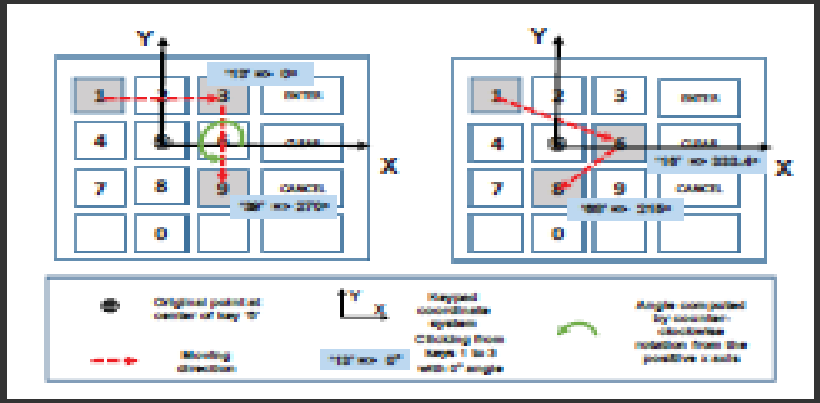
Chen Wang
Department of ECE
Stevens Institute of Technology
Hoboken, NJ, USA
cwang42@stevens.edu

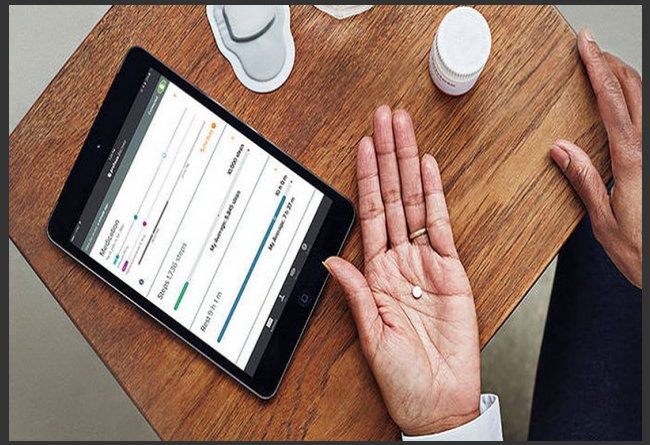
Xiaonan Guo
Department of ECE
Stevens Institute of Technology
Hoboken, NJ, USA
xguo6@stevens.edu

Yan Wang
Department of CS
Binghamton University
Binghamton, NY, USA
yanwang@binghamton.edu

Yingying Chen
Department of ECE
Stevens Institute of Technology
Hoboken, NJ, USA
yingying.chen@stevens.edu

Bo Liu
Department of ECE
Stevens Institute of Technology
Hoboken, NJ, USA
bliu11@stevens.edu





Transmit personal data from wearables to participants' smartphones via Bluetooth to clinical trial dataset

2019: 15% of clinical trials incorporate wearables

2025: 70% of clinical trials will incorporate wearables

Critical Path Institute's Consortium Publication:

Selection and Validation of Wearable Devices

VALUE IN HEALTH 21 (2018) 631–639

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jval

ELSEVIER

Value in Health

CrossMark

Selection of and Evidentiary Considerations for Wearable Devices and Their Measurements for Use in Regulatory Decision Making: Recommendations from the ePRO Consortium

Bill Byrom, PhD[1,*], Chris Watson, PhD[2], Helen Doll, DPhil[3], Stephen Joel Coons, PhD[4], Sonya Eremenco, MA[4], Rachel Ballinger, PhD[5], Marie Mc Carthy, MBA[5], Mabel Crescioni, DrPh[4], Paul O'Donohoe, MSc[6], Cindy Howry, MS[7], on behalf of the ePRO Consortium

[1]ICON Clinical Research, Marlow, Buckinghamshire, UK; [2]ERT, Nottingham, Nottinghamshire, UK; [3]ICON Clinical Research, Abingdon, Oxfordshire, UK; [4]Critical Path Institute, Tucson, AZ, USA; [5]ICON Clinical Research, Dublin, Ireland; [6]CRF Health, London, UK; [7]assiTek, Scottsdale, AZ, USA

ABSTRACT

Background: Wearable devices offer huge potential to collect rich sources of data to provide insights into the effects of treatment interventions. Despite this, at the time of writing this report, limited regulatory guidance on the use of wearables in clinical trial programs has been published. **Objectives:** To present recommendations from the Critical Path Institute's Electronic Patient-Reported Outcome Consortium regarding the selection and evaluation of wearable devices and their measurements for use in regulatory trials and to support labeling claims. **Methods:** The evaluation group was composed of Critical Path Institute's clinical outcome assessment (COA) scientists and COA specialists from pharmaceutical trial eCOA solution providers, including COA development and validation specialists. The resulting recommendations were drawn from a broad range of backgrounds, perspectives, and expertise that enriched the development of this report. Recommendations were developed through analysis of existing regulatory guidance relating to COA development and use in clinical trials, medical device certification/clearance regulations, literature-reported best practice, and practical experience of wearable technology application in clinical trials. **Results:** We identify the essential properties of fit-for-purpose wearables and propose evidence needed to support their use. In addition, we overview the activities required to establish clinical endpoints derived from wearables data. **Conclusions:** Using this framework, we believe there is enough current understanding to promote the appropriate use of wearables in study protocols. We hope this will provide a basis for discussion among clinical trial stakeholders and catalyze the development of more robust regulatory guidance.

Keywords: clinical outcomes, clinical trial endpoints, clinical trials, performance outcomes, remote monitoring, validation, wearables.

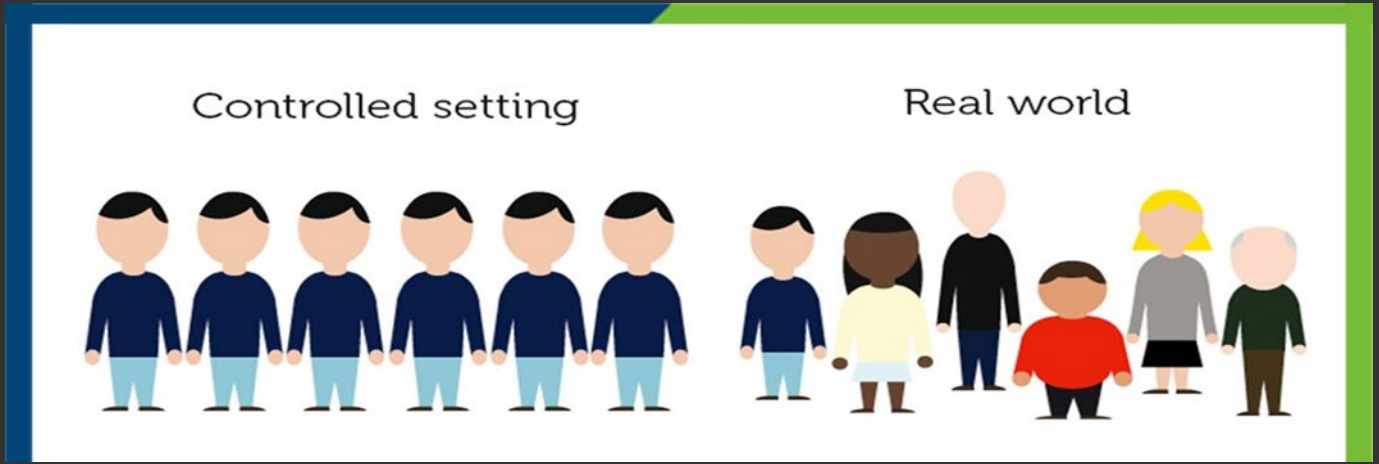
Introduction

Miniaturization of sensors and circuitry has given rise to huge proliferation in the development and commercialization of wearables and sensors with application to health and wellness. Examples are wide-ranging and include patches for electrocardiogram monitoring, wrist-worn devices for sleep assessment, and sensors with subcutaneous probes for continuous glucose monitoring. Activity monitors with their associated mobile applications and software are increasingly popular among those wishing to improve fitness or manage weight through regular exercise regimens.

Responding to this growing market of novel and interesting wearables and sensors, the biopharmaceutical industry is actively interested in knowing how to harness these devices to enable greater information to be learnt about the effects of treatments during drug development. Despite the promise of this technology, there is uncertainty regarding the regulatory acceptability of data collected in this way—specifically in understanding what evidence should be available and considered when selecting an appropriate device for use in a clinical trial to ensure adequate precision, accuracy, and reliability of data collected and the nature of evidence required to demonstrate appropriateness and clinical relevance of new endpoints derived from the data.

The purpose of this report was to propose a set of recommendations for the biopharmaceutical industry in relation to the selection of and evidentiary considerations for wearable devices and sensors and their outcome measures for use in regulatory clinical trials. These recommendations are based on the current literature, regulatory guidance available to date, and expert consensus of the member firm representatives of the Electronic Patient-Reported Outcome Consortium, a technology industry research group with the Critical Path Institute as its managing member.

Byrom, Bill et al. Selection of and Evidentiary Considerations for Wearable Devices and Their Measurements for Use in Regulatory Decision Making: Recommendations from the ePRO Consortium. *Value in Health 21:*6, June 2018.



- Meaningful data
- New findings that connect lifestyle with disease
- Lower costs (site, time, tests)
- Generate huge volumes of data

Unintended data

- **Additional data points** collected from wearables by virtue of the transmission process → Unintended Data
  - **Issue**: Collect, store, and reuse sensitive categories of personal data - Genetic, Biometric, Health – that may not be relevant to stated research purpose
  - Beyond individual identification and geolocation
  - Little and conflicting guidance from GDPR and CCPA

Key principles in GDPR

1. Personal data can only be collected for a **specific purpose**.

2. The person must be **informed of and consent** to the purpose for which their data is collected.

3. Only as much **data as is necessary** to achieve that purpose should be collected.

4. The collected data **must be deleted** at the request of the participant, or when it is no longer needed for the purpose which it was collected.

Research occupies a privileged position within GDPR

Broad definition of research – "technological development and demonstration, fundamental research, applied research, privately funded research" (Recital 159).

"Organizations that process personal data for **research purposes may avoid restrictions** on secondary processing" (Article 6(4); Recital 50).

"As long as there are **appropriate safeguards** for the rights and freedoms of the data subject, organizations may **override a data subject's right to object to processing and to seek erasure** of personal data" (Article 89).

Appropriate safeguards

Ensure that only access to personal data **necessary for the research purposes** in accordance with the **Principle of Data Minimization** (Article 5).

Principle of Data Minimization
Limit personal data collection, storage, and usage to data that are **relevant, adequate, and absolutely necessary** for carrying out **stated purpose** for why data is being processed.

Further exemptions for research

- "It is often not possible to **fully identify the purpose** of personal data processing for scientific research purposes at the time of data collection" (Recital 33).

- *But see* "Well-described purpose" must be included in the consent to comply with the GDPR (Working Party Draft Guidelines at 27).

- **Nation-specific research exemptions** for additional rights provided there are appropriate safeguards (Article 9).

CCPA and Research Exemption

Limits definition of research to only federally sponsored research.

“Permit access only to the minimum necessary personal information needed for the research project.”

Certain rights (e.g., deletion) not apply to “research”

How to reconcile the deliberate aims of GDPR and CCPA with a research exemption?

A better understanding of how the GDPR and CCPA will evolve is needed before future regulation is passed.

Role of collective action? GDPR allows data subjects the right to a consumer protection body to bring claims on their behalf (Article 70) … but for research?

The NEW ENGLAND JOURNAL of MEDICINE

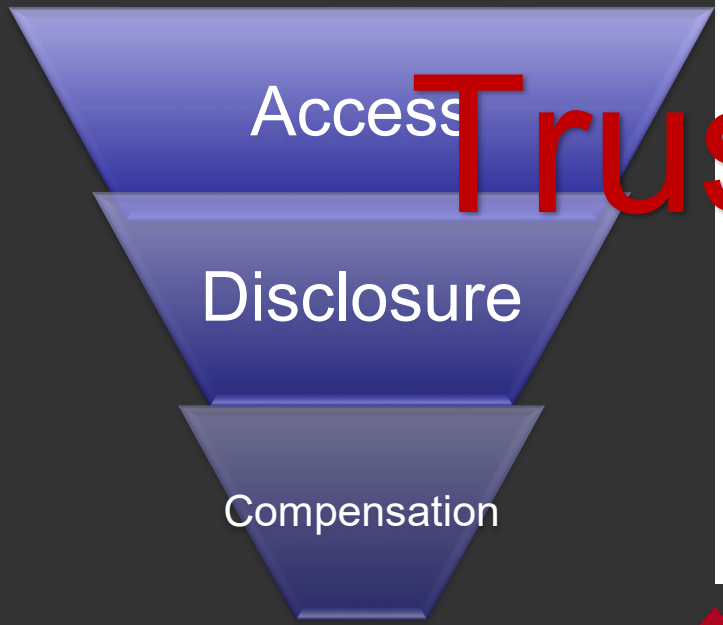
Clinical Trial Participants' Views of the Risks and Benefits of Data Sharing

"In our study, ***few clinical trial participants had strong concerns about the risks of data sharing****. Provided that adequate security safeguards were in place, most participants were willing to* ***share their data for a wide range of uses."***

Michelle M. Mello, et al. Clinical Trial Participants' Views of the Risks and Benefits of Data Sharing. N Engl J Med 378:23, June 7, 2018.

Research Participant

Responsive to what participants <u>value:</u>



Trust

PATIENTS & CONSUMERS

By Consuelo H. Wilkins, Brandy M. Mapes, Rebecca N. Jerome, Victoria Villalta-Gil, Jill M. Pulley, and Paul A. Harris

Understanding What Information Is Valued By Research Participants, And Why

ABSTRACT There is growing public demand that research participants receive all of their results, regardless of whether clinical action is indicated. Instead of the standard practice of returning only actionable results, we propose a reconceptualization called "return of value" to encompass the varied ways in which research participants value specific results and more general information they receive beyond actionable results. Our proposal is supported by a national survey of a diverse sample, which found that receiving research results would be valuable to most (78.5 percent) and would make them more likely to trust researchers (70.3 percent). Respondents highly valued results revealing genetic effects on medication response and predicting disease risk, as well as information about nearby clinical trials and updates on how their data were used. The information most valued varied by education, race/ethnicity, and age. Policies are needed to enable return of information in ways that recognize participants' differing informational needs and values.

Consuelo H. Wilkins (consuelo.wilkins@vumc.org) is the vice president for health equity, Vanderbilt University Medical Center, and an associate professor in the Department of Medicine, Vanderbilt University Medical Center, and the Department of Internal Medicine, Meharry Medical College, all in Nashville, Tennessee.

Brandy M. Mapes is a senior project manager in the Vanderbilt Institute for Clinical and Translational Research, Vanderbilt University Medical Center.

Rebecca N. Jerome is a manager of translational research in the Vanderbilt Institute for Clinical and Translational Research, Vanderbilt University Medical Center.

Victoria Villalta-Gil is a senior research specialist in the Meharry Vanderbilt Alliance.

Jill M. Pulley is executive director of the Vanderbilt Institute for Clinical and Translational Research, Vanderbilt University Medical Center.

Paul A. Harris is director of the Office of Research Informatics in the Vanderbilt Institute for Clinical and Translational Research, Vanderbilt University Medical Center.

There has been considerable debate about whether or not to return individual research results to participants. Because the purpose of research is to generate generalizable evidence and not to guide individual clinical care or health management, researchers historically have not been obliged to return individual results. Views on this have evolved, because of the increasing availability of genetic test results as well as public demands for access to personal data.[1–3] However, considerations on whether or not to return results have largely focused on whether the results would affect clinical decision making. Often, little regard has been paid to participants' perspectives on the personal utility of the results.

Concerns about the validity and usefulness of research results is considered a primary reason for not returning results to participants.[4–6] There is also concern for potential risks of returning results, including the costs and burden of subsequent clinical evaluations, potential harm resulting from unnecessary procedures, emotional stress to the participant and family when results are uncertain, and privacy breaches.[5,6,7] Primary care physicians may also be burdened with the responsibility of explaining research results of unclear significance.[8] Consequently, many researchers have not returned results unless a clear and urgent action is warranted (duty to warn" or inform) or the results can be easily interpreted and acted upon. Lack of training in how to effectively communicate results and limited resources to share results also contribute to researchers' hesitance to return results.[4]

Public perceptions on who owns data[9] and views that participants should be partners in research[10] have called into question the prevailing practices regarding return of results. Mounting evidence shows that participants want to learn their individual research results and that

Thank you

trsklar@email.arizona.edu