



**Knobbe Martens**

# Respect and Protect: Intersection of Med Devices, AI, and Data Privacy

February 10, 2020

Curtis Huffmire

6<sup>th</sup> Annual International Symposium on  
Technology in Medical Data and  
Devices

3:15 PM

# Trends in Med Device AI and Data Privacy

## Trends in Med Device AI and Data Privacy

---

- Med Devices are sensing and collecting more data
- Med Devices are connected and transmitting more data
- Med Devices are provided access to more data
- Med Devices are learning and improving outcomes using data
- Data is becoming increasingly valuable
- Companies and Governments are respecting and protecting data

## Trends in Med Device AI and Data Privacy

---

- Respecting Data
  - Patients have a right to privacy and control of their data
- Protecting Data
  - Companies and Governments have responsibilities to secure data
- Data Privacy and Data Security are essential aspects of a Med Device company's success
  - Strong Data Privacy and Security Policies lead to increased value
  - Weak Data Privacy and Security Policies lead to increased losses

## Cost of Data Breach

Average total cost of  
a data breach:

**\$3.86 million**

Average total one-year  
cost increase:

**6.4%**

Average cost per lost or  
stolen record:

**\$148**

One-year increase in  
per capita cost:

**4.8%**

Likelihood of reoccurring  
material  
breach over the next 2 years:

**27.9%**

Average cost savings with an  
Incident Response team:

**\$14 per record**

What your personal  
data is worth to a  
hacker (per record)

- \$10 Name, Address & Email
- \$50 Drivers license
- \$50 Credit/Debit Card
- \$3 Netflix password
- \$100 Bank password
- \$1000 Bank password (balance >\$15k)
- \$1000 Complete medical record
- \$300 Average medical record

The incentives for hackers are great

The personal data of a  
US resident is worth  
about

**\$2000 — \$3000**  
per year

*Ponemon Institute; 2018 Cost of a Data Breach Study: Global Overview*

How should my Med Device Co respect and protect data?

## How should my Med Device Co respect and protect data?

---

- Companies should fully embrace data privacy and security
  - Take responsibility to respect the customer/patient re use of data
  - Take responsibility to secure the valuable customer/patient data
  - Comprehensive privacy and security plans will pay off long term
- Jurisdictions have new and developing laws
  - Understand the laws
  - Comply with the laws

## Hypothetical Med Device Co makes standard pacemakers

---

- What kinds of data are involved?
  - Basic customer info?
    - Name, Address, Phone, Age, Birthdate?
    - Web IP address, shopping preferences?
  - Patient related data?
    - Health history? Mobile data? Heart rate?



- What are basic requirements for Data Privacy and Security?



## Data Privacy 101

---

- Broad term that encompasses many areas of law and issues
  - **Common law rights to privacy**
    - False light, intrusion, appropriation, and public disclosure of private facts
  - **Statutes** related to certain industries/sectors (e.g., Telephone Consumer Protection Act, Fair Credit Reporting Act, Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, Health Insurance Portability and Accountability Act of 1996, etc.)
  - **Data breach notification** laws (all 50 states)
  - **Comprehensive Data Rights Statutes**
    - General Data Protection Regulation (GDPR)
    - California Consumer Privacy Protection Act (CCPA)
    - No U.S. federal comprehensive data privacy law
    - Closest is Section 5(a) of the Federal Trade Commission Act, which prohibits “unfair or deceptive acts or practices”

## CCPA v. GDPR



- Requires consent from the individual
- Wide definition of personal information including browser history, purchase behaviour, site/app interactions
- Allows for opt-out of collection/use
- Fines potentially in the millions of dollars
- Private right of action, class suits
- Extraterritorial effect on business



- Has a legitimate interest component
- Defines PII and sensitive information
- Default to opt-in for collection/use
- Fines potentially in the millions of dollars
- Public complaints to an enforcement body to address
- Extraterritorial effect on business

## Personal Rights under the GDPR

---

- Right to Access Personal Data
- Right to Rectification
- Right to Erasure
- Right to Restrict Data Processing
- Right to Be Notified
- Right to Data Portability
- Right to Object
- Right to Reject Automated Individual Decision Making

# CCPA – California Consumer Protection Act – Summary

---

## Who?

Any for-profit businesses conducting business in California that collects or processes personal consumer data of California residents **AND** also meets one of:

- Revenue \$25MM+ OR
- Data of 50,000 Californian consumers, OR
- Derive 50%+ of revenue selling consumer data



**More than 1,000,000**

businesses will be affected by the CCPA

## What?

CCPA expressly focuses on: Preventing ‘misuse’ of Californians’ consumer data through increased transparency.

## New Consumer Data Rights:

1. To **Request** knowledge (visibility) of their data used by the business
2. To **Delete** their data used by the business
3. To **Opt-out of the sale** of their data

## Penalties

Enforcement will levy fines (up \$7,500/event) injunctive, or class action relief/rights

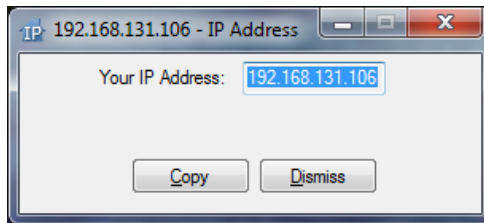
# Expansive Definition of Personal Information (PI)

**“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.”**

email address  
*FredYellowtail@work.com*

**HELLO**  
my name is

Name



Username  
Online identifiers

Password [Show](#)

[Log In](#)

☐ Keep me logged in

[Forgot username?](#) [Forgot password?](#)



search history|

search history

search history **youtube**

search history **safari**

## Discovery Mode / Data Mapping

- First step in privacy compliance
- Identify collection, flow and retention of PI
- Identify purpose of PI
- User friendly worksheet available to assist
- Third party vendors offer software solutions
- Recommend naming DPO or lead
- Review and update vendor agreements

### II. SOURCES TO CONSIDER

When reviewing the questionnaire, please consider all possible sources in your operations. These sources may include your company, subsidiaries, sub-contractors, parent companies, service providers (e.g., hosting services, billing services, and analytic services), third-party vendors, employees, or customers. Each department of your company may implicate data privacy including human resources, finance, marketing, development, testing, and procurement.

### III. QUESTIONS

<b>Section 1 – Identifying Personal Information Under The CCPA</b> <i>This section helps identify the collection of data that triggers obligations under the CCPA.</i>	
<p>1. <u>What data do you collect from or about consumers?</u></p> <p>a. Please list each type of data from or about <u>consumers</u> that you <u>collect</u>, with reference to the broad definition of “collects,” “collected,” and “collection” above (see page 2). [Note: While the CCPA is limited to protecting <u>personal information</u>, please provide an exhaustive list of all data about <u>consumers</u> (which includes employees under the current statute) that you <u>collect</u> so that we may evaluate whether any particular data is or is not covered by the CCPA.]</p> <p>b. For each answer to Question 1(a), please state the purposes (including commercial purpose or <u>business purpose</u>) for which the category of <u>collected</u> data is to be used.</p>	
<p>2. Are there any types of data (listed in response to Question 1(a)) that include information that is <u>publicly available</u> at the time of or before <u>collection</u>?</p>	
<p>3. If you answered “YES” to Question 2, please explain the circumstances of the <u>public availability</u> and your <u>collection</u> of the data.</p>	

## Consumer Rights in CCPA

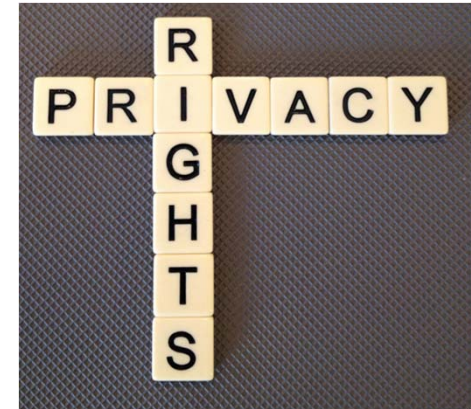
CA consumers can make a verifiable request regarding:

1. Right to know/access what PI is being collected and sold
2. Right to deletion
3. Right to opt-out

Businesses have 45 days to respond


### How to comply:

- Set up a toll-free telephone # for requests
- Train employees to manage toll-free # or retain outside vendor to manage
- Train existing customer relations team about where to direct CCPA inquiries
- Create web page where consumers can submit requests
- Prepare template responses / ensure capabilities to provide data in portable form
- Compliance tracking



## Compliance Road Map

---

- 
- Create internal data privacy team, including point person, with relevant stakeholders
  - Obtain cyber insurance
  - Retain outside counsel
  - Consider retaining a company to assist with operations/IT
  - Conduct inventory of data collection and use
  - Prepare and update privacy policies and procedures
  - Prepare and update vendor agreements
  - Set up compliance mechanism for consumer access requests
  - Train personnel
  - Ensure PI is protected with adequate and reasonable security measures
  - Regular audits of privacy and security programs



## Hypothetical Med Device Co makes AI-based pacemakers

---

- What kinds of data are involved?
  - Updates of algorithms?
    - Data of 1000s of other patients?
  - Raw patient data?
    - AI engine onboard?
- How does AI change the analysis?



- What are basic requirements for Data Privacy and Security?

## How should my Med Device Co respect and protect AI related data?

---

- Promoting AI and capturing its benefits for the health care systems depends on access to sensitive patient data.
- Ensuring that privacy protections are in place is essential.
- Assuring the right to privacy of citizens while facilitating access to personal data for research is a major challenge that is still being considered by many jurisdictions to benefit from many opportunities of AI technologies in health care.

## Personal Rights under the GDPR

---

- Right to Access Personal Data
- Right to Rectification
- Right to Erasure
- Right to Restrict Data Processing
- Right to Be Notified
- Right to Data Portability
- Right to Object
- Right to Reject Automated Individual Decision Making

## How should my Med Device Co respect and protect AI related data?

---

- Can data be de-identified and/or made anonymous?
- For GDPR, what legal basis is relied on? Dealing with special category data? If so, what Article 9 condition applies?
- Dealing with any data collected pre-GDPR?
- Need to rely on consent? If so, is language sufficiently clear and specific?
- Adequate privacy notice?
- What are the particular rights at stake and how is the obligations to protect these rights going to be met?

## Privacy By Design

---

- Proactive Not Reactive; Preventative Not Remedial
- Privacy As Default Setting
- Embedded Privacy in Design
- Full Functionality – Positive-Sum Instead of Zero Sum
- Transparency and Visibility – Make it Open
- End-to-End Security – Full Lifespan Protection
- Respect for the Privacy of the User – Make it User-Centric

## Privacy By Design – AI Considerations

---

- Educate Engineers about Privacy
- Control Access to Data
- Minimum Data for Collection and Processing
- Strong De-Identification – Anonymous Data
- Beware of Quasi-Identifiers
- Ability to Handle Erasure and Rectification Access
- Explain the Logic – White Box vs. Black Box



Knobbe Martens

Thank you!

Curtis Huffmire

[Curtis.Huffmire@knobbe.com](mailto:Curtis.Huffmire@knobbe.com)