



Knobbe **Martens**

Protect and Respect: Legal Protections for Medical Devices & Data

September 14, 2022

Curtis Huffmire

7th Annual International Symposium on
Technology in Medical Data and
Devices

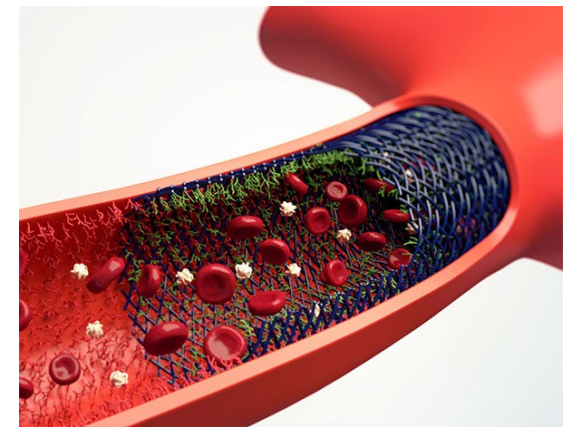
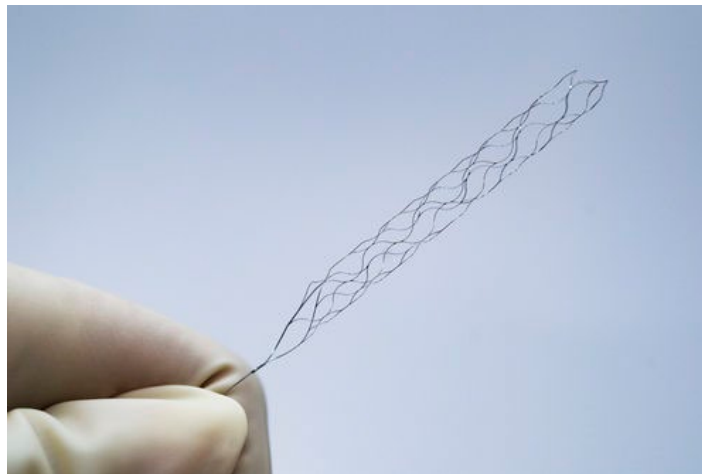
Irvine, CA

Overview

- Recent Deals in the Medical Device Space
- Increasing Value by focusing on both IP and Data Protections
- Protecting Innovation with Patents and other IP
- Respecting Privacy and implementing Data Controls

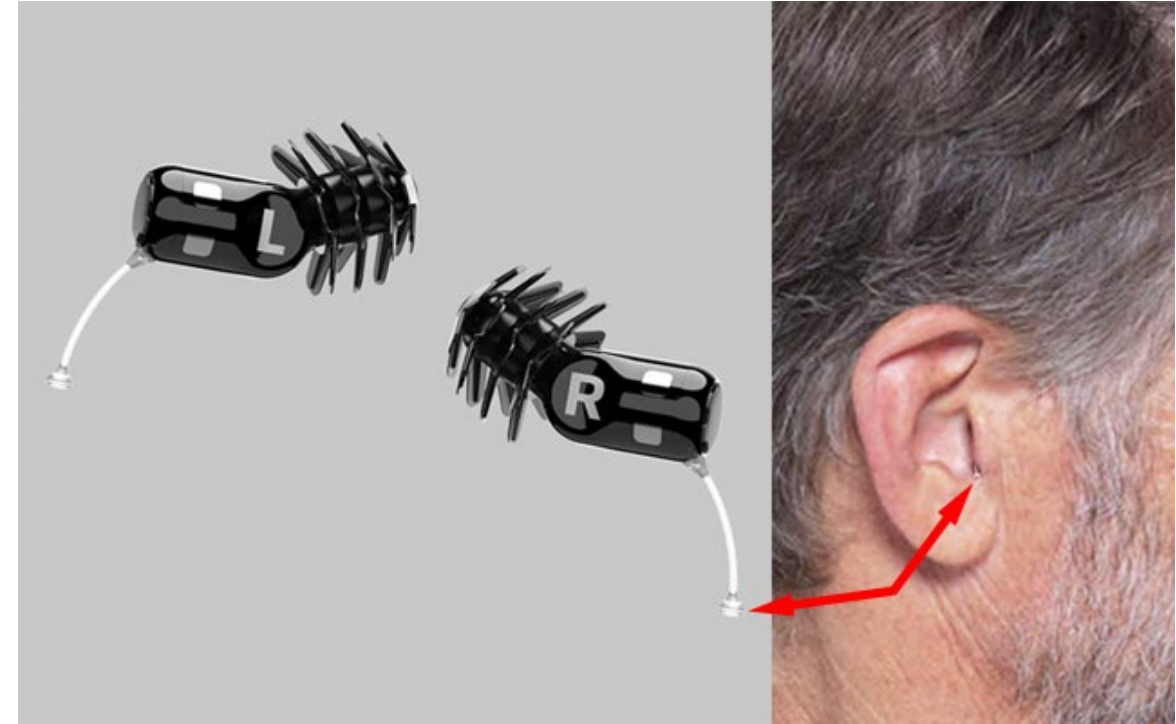
Recent Medical Device Deals in the News

- Wallaby Acquires German Neurovascular Leader Phenox - \$543M
 - Neurovascular devices to treat ischemic and hemorrhagic strokes
 - One of the largest cross-border transactions in the medical device industry globally in recent years
 - Global leader in providing a wide range of neurovascular technologies and solutions to its customers and patients around the world, including in the U.S., China, Europe, Japan and other international markets.



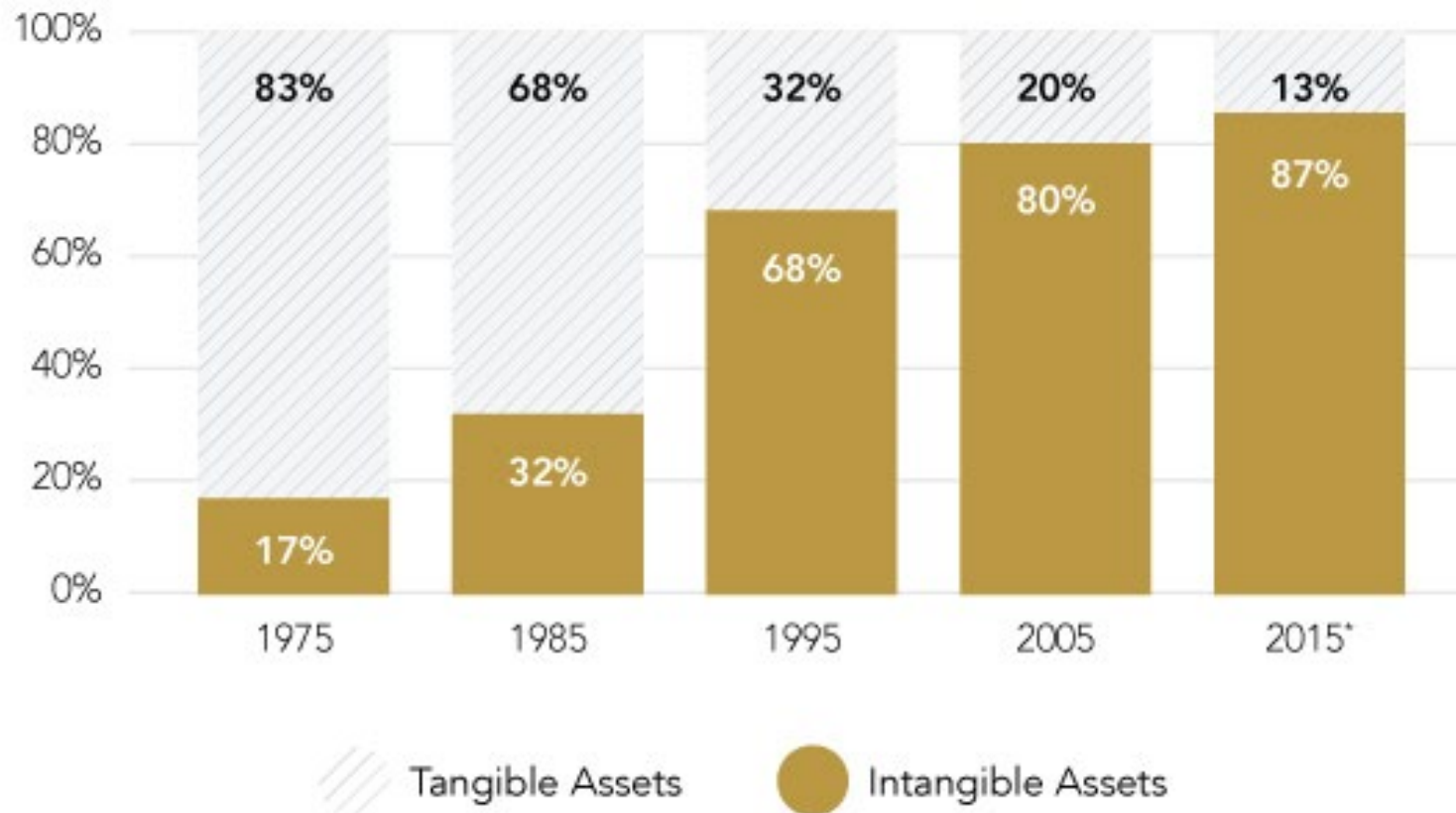
Recent Medical Device Deals in the News

- Eargo secures \$100M investment from Patient Square Capital
 - Eargo hearing aids are virtually invisible, rechargeable, completely-in-canal, FDA regulated and indicated to compensate for mild to moderate hearing loss.
 - According to some aspects, the device can have an accelerometer and a power control module to receive input data in order to make a determination to autonomously change a power mode for the hearing aid based on movement.



Businesses Are Increasingly Valued By Intangible Assets

COMPONENTS *of* S&P 500 MARKET VALUE



IP Valuation

IP depends on other assets and resources in order to generate economic benefits



Patents Are Critical Assets In Medical Device Valuations and Acquisitions

MILESTONES TO ACQUISITION

- 1 PROOF OF CONCEPT
- 2 PATENT PROSECUTION
- 3 FDA APPROVAL
- 4 CLINICAL TRIALS
- 5 EXIT: STRATEGIC PARTNERSHIP



Don't Neglect Data Security and Privacy



- 1 in 4 will experience a data breach.
- Cost of a breach can be about \$4M or more on average.
- Don't depend on privacy compliance alone—Be Proactive!

Protect Your Innovation with a Patent Fortress

- Control the Core
- Expand the Wall
- Prepare for Battle



Control the Core – Evaluate Your Core Patent Position in an IP Audit

- Confirm ownership properly documented
- Foster communication between teams to confirm marketable features are protected by patent claims
- Incentives to encourage recording inventions



Control the Core

- Secure rights with solid IP Agreements
 - Hire IP counsel for IP agreements
 - Execute strong NDA's before disclosing to others
 - Secure broad assignment agreements with all inventors
 - Be very careful with co-development agreements
 - Seek to own all IP
 - If not possible, define categories very carefully for ownership or use
 - Do not try to avoid the controversy through “co-ownership” of IP

- Obtain meaningful patents
 - File early
 - Perform prior art searching and cite all prior art to examiner
 - Use expedited examination
 - Do not say conflicting things at Patent Office and FDA
 - Keep foreign options open in relevant markets

Expand the Wall – File Continuing Patent Applications of Strategic Scope

- “IP Round-up”
- Foster communication about areas of future growth or expansion and direct patents to the space early on
- Encourage Provisional Patent Applications
- Protect Alternatives



- Employ sophisticated patent claim strategies
 - Seek diverse coverage
 - devices and methods
 - Use varying claim scope and different specifications
 - Avoid claiming “too much”
 - Limit contextual structure
 - Be careful with reusable and disposable components
 - Use functional language
 - Always keep a continuation pending

Prepare for Battle – Develop Strategic Offensive and Defensive Plans

- Conduct regular patent searching
- Foster communication about what is observed from competition in market
- Obtain opinions of counsel regarding third party patents of risk
- Craft claims to block competitor advancement



Prepare for Battle

- Do freedom-to-operate searching and analysis
 - It is expensive but can dramatically enhance your company's valuation
 - Design-around where possible
 - Develop reliable non-infringement or invalidity arguments
 - Be careful about waiving attorney-client privilege in diligence discussions
 - Be wary of approaching IP owners to seek licenses

- Trade Secrets
 - Not a substitute for a patent
 - But can be very powerful in right circumstances
 - Must be kept secret; not easily reverse-engineered
 - Must be able to describe without disclosing secret
 - Strong contracts and diligent in keeping it secret

Prepare for Battle

- Don't forget other IP issues
 - Trademarks
 - Copyrights
 - Domain names
 - Data privacy

Trends in Med Device and Data Privacy

Trends in Med Device 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 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

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



More than 1,000,000

businesses are affected by the CCPA

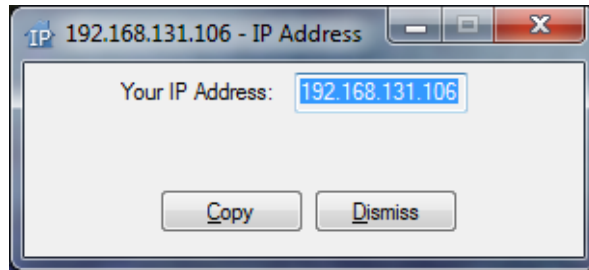
Penalties

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



Username
Online identifiers

Password Show

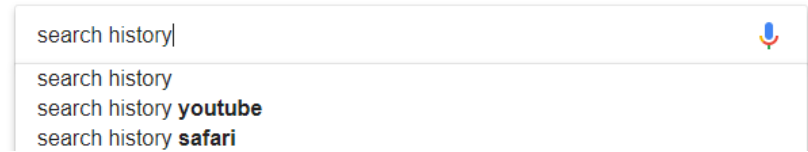
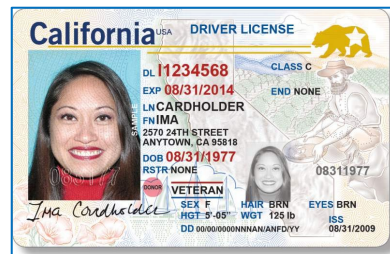
Log In

Keep me logged in

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



Name



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

Section 1 – Identifying Personal Information Under The CCPA <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

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

Breach Prep – Be Proactive

- Identify and locate your data assets and understand the flow of data assets through your organization
- Institute tiered security measures to protect your data assets
- Adopt security measures consistent with recognized guidance and objectively assess the effectiveness
- Monitor your networks for intrusion and fix what you find
- Train employees to manage data responsibly
- Consider creating a role of Data Privacy Officer; decide who is responsible for organizing preparedness
- Create an Incident Response Plan; ensure key players have a printed copy of the plan
- Test, prove, and improve your Incident Response Plan
- Continue to update your Incident Response Plan to reflect necessary changes in organization, employees, contacts, etc.
- Align other internal policies with your Incident Response Plan
- Consider cyber insurance and understand your insurance policies; verify that third-party vendors have sufficient cyber insurance coverage
- Develop proactive relationships with outside counsel, investigative cyber security firms, relevant law enforcement agencies, and a PR consultant in the event of an incident; include contact information for key contacts in the Incident Response Plan

How to Respond to Breach

- **Initial Assessment**

- Scope, extent and nature of the incident; Is it malicious?
- Initiate incident response plan, assemble stakeholders and counsel

- **Internal Investigation (forensic, interviews)**

- Minimize continuing damage
- Collect and preserve data (network image, logs, notes, and records)
- Keep records of ongoing attacks

- **Notifications**

- Board of Directors, management team, key personnel
- Law enforcement, government agencies
- Partners, third parties (vendors)

- **Prepare for:**

- Consumer data breach notification
- Government investigations (State AGs, FTC, SEC, etc.)
- Negative publicity; Ancillary litigation

Data Privacy Services

➤ **Our Services**

- Determine if certain data privacy laws apply to the client, and potential exemptions
- Compliance with federal, state and international laws
- Audit privacy and security programs and procedures
- Prepare or update privacy policies and procedures in light of new and emerging laws (e.g., CCPA)
- Train employees regarding compliance with data privacy laws
- Audit vendor contracts to ensure key provisions included in the agreements related to data privacy issues
- Data mapping (what personal information is collected, purpose, who its shared with, where is it stored etc.)
- Counseling regarding data breaches and responses to same
- Data privacy assessment for launch of new products that collect personal information (Internet of Things)
- Prepare compliance mechanism for consumer access requests
- Marketing and behavior analytics compliance
- Privacy by design
- Assist clients with cybersecurity due diligence reviews
- Advice to clients under investigation by federal/state agencies to properly address inquiries or investigations
- Handle litigation involving data breaches and data protection laws



Knobbe **Martens**

Thank You!

Curtis Huffmire

Curtis.Huffmire@knobbe.com