



Mastering Tomorrow's Healthcare Tech

A Cutting-Edge Approach to Regulatory,
Compliance, and Privacy Demands

Thursday, November 9th, 2023

Agenda

- 9:00 – 9:05 AM Program Introduction by Mark Gardner
- 9:05 – 10:00 AM Compliance Considerations in High-Tech Healthcare
Speakers: Amanda Johnston & Cord Willhöeft
- 10:00 – 10:45 AM Preparation and Opportunity: Managing Privacy and Cybersecurity Risks in Connected Devices
Speakers: Paul Rothermel & Oliver Sueme
- 10:45 – 11:00 AM BREAK
- 11:00 – 11:45 AM FDA Engagement Strategies: Harnessing AI and Connected Devices in Medical Innovation
Speakers: Nate Downing & Cord Willhöeft
- 11:45 – 12:30 PM Panel Discussion
Moderator: Mark Gardner
Panelists: Jeff Dennis, Sara Kerrane & Sushana Vijayakumar

Presenter Introduction

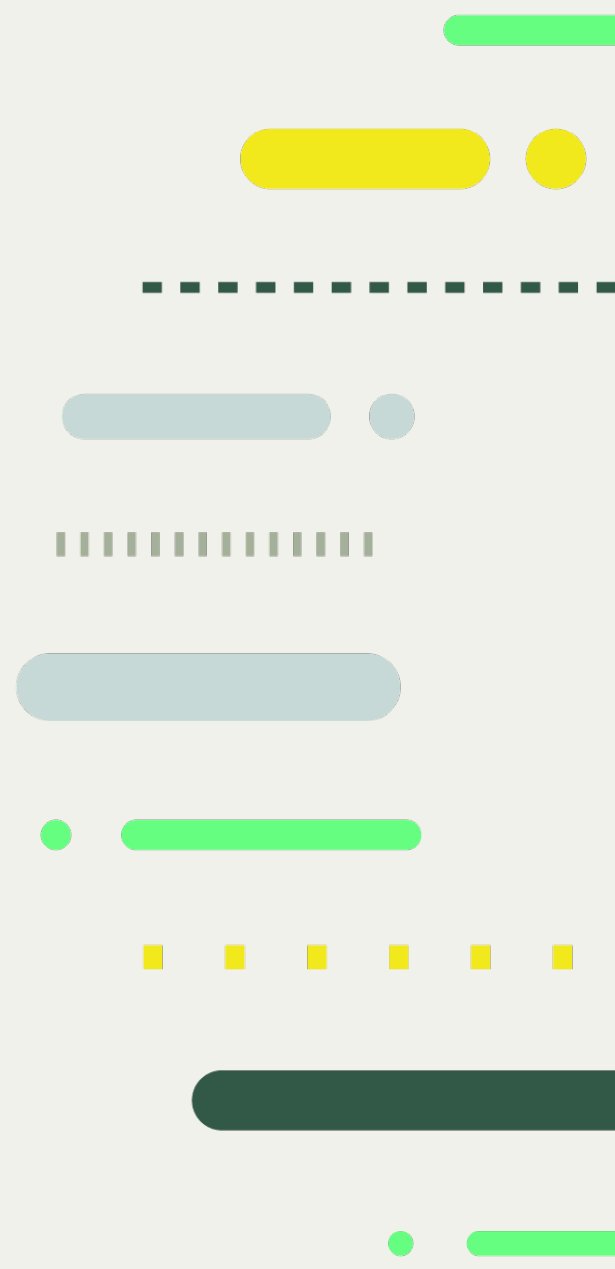


Mark founded Gardner Law, an FDA law firm that specializes in regulatory, compliance, and privacy matters. His specialties include guiding clients through complex FDA matters, performing due diligence for buyers and sellers, assessing sales and marketing programs and commercial transactions, designing and implementing compliant ways to interact with healthcare providers, facilitating government transparency reporting, and auditing and investigating company activities for compliance with the law. Mark works with regulators at the FDA, CMS, and OCR, and with law enforcement at the DOJ and OIG.

Mark Gardner, J.D., M.B.A.

Directing Attorney
mgardner@gardner.law
Phone: 612.382.7584

GARDNER
FDA LAW FIRM



Program Introduction

- Program is being recording and the recording will be available post-event.
- Slides are available during the presentation virtually via the handout window on the control panel.
- Remote participants: Please submit questions via the question function on the control panel.
- CLE credits: 3.0 credits have been approved by the Minnesota Board of Continuing Legal Education. Please request a CLE certificate to self report in other states from office@gardner.law.





Compliance Considerations in High-Tech Healthcare

Amanda Johnston

Thursday, November 9th, 2023

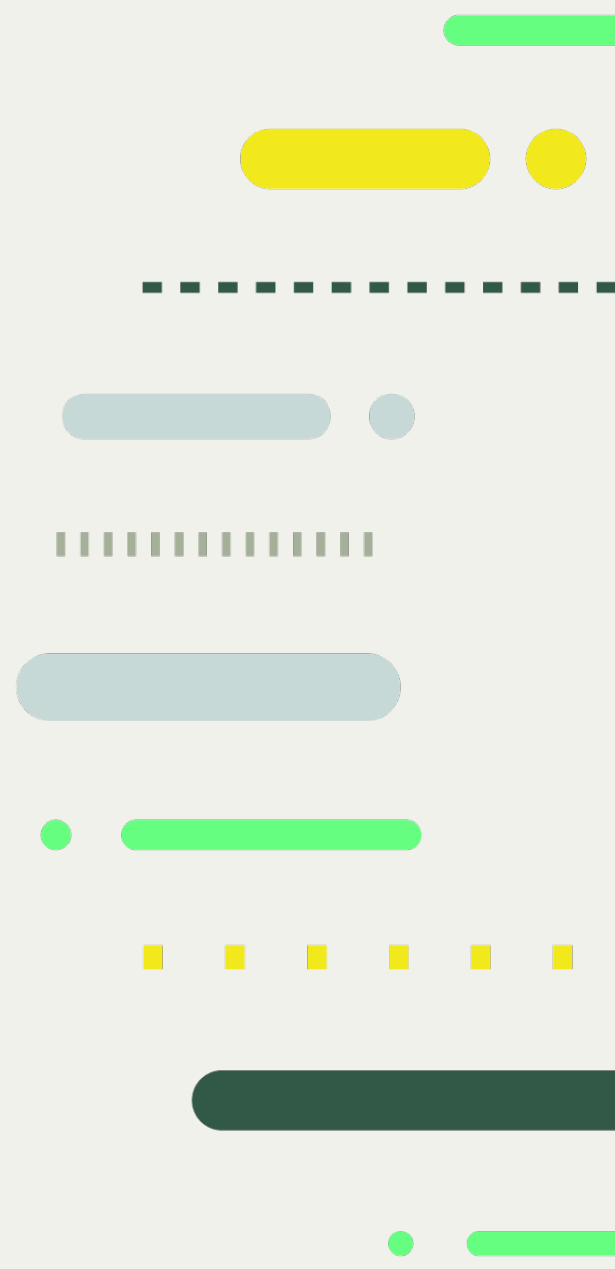
Presenter Introductions



Amanda Johnston, J.D.
Managing Attorney
ajohnston@gardner.law
Phone: 763-639-6951

GARDNER
FDA LAW FIRM

Amanda Johnston is a distinguished FDA attorney with expertise in counseling medical device and pharmaceutical companies on FDA law, regulatory submissions, healthcare compliance programs, and healthcare fraud and abuse laws. With an impressive background spanning several in-house legal, regulatory, and compliance roles within the medical device industry, Amanda brings an exceptional understanding of business and industry dynamics to her practice. Her extensive experience includes serving as interim compliance officer at a global medical device company, overseeing 130+ FDA submissions, compliance program implementation, and helping commercial teams navigate healthcare fraud and abuse laws.



Agenda

- Introduction
- Overview of applicable laws
- Compliance considerations
 - Payment, Reimbursement
 - Product and Services
 - Durable Medical Equipment (DME)
 - Cybersecurity
 - Telemedicine
 - Clinical Laboratory Testing



High-Tech Healthcare Examples



- Smart inhaler
- Robotic surgery
- Wearable biosensors
- Precision medicine
- Virtual reality
- Telehealth
- Artificial organs
- Remote patient monitoring
- Image analysis
- Surgery planning
- Virtual assistants
- AI-assisted telemedicine
- Diagnostic imaging
- Fitness trackers
- Wearable monitors

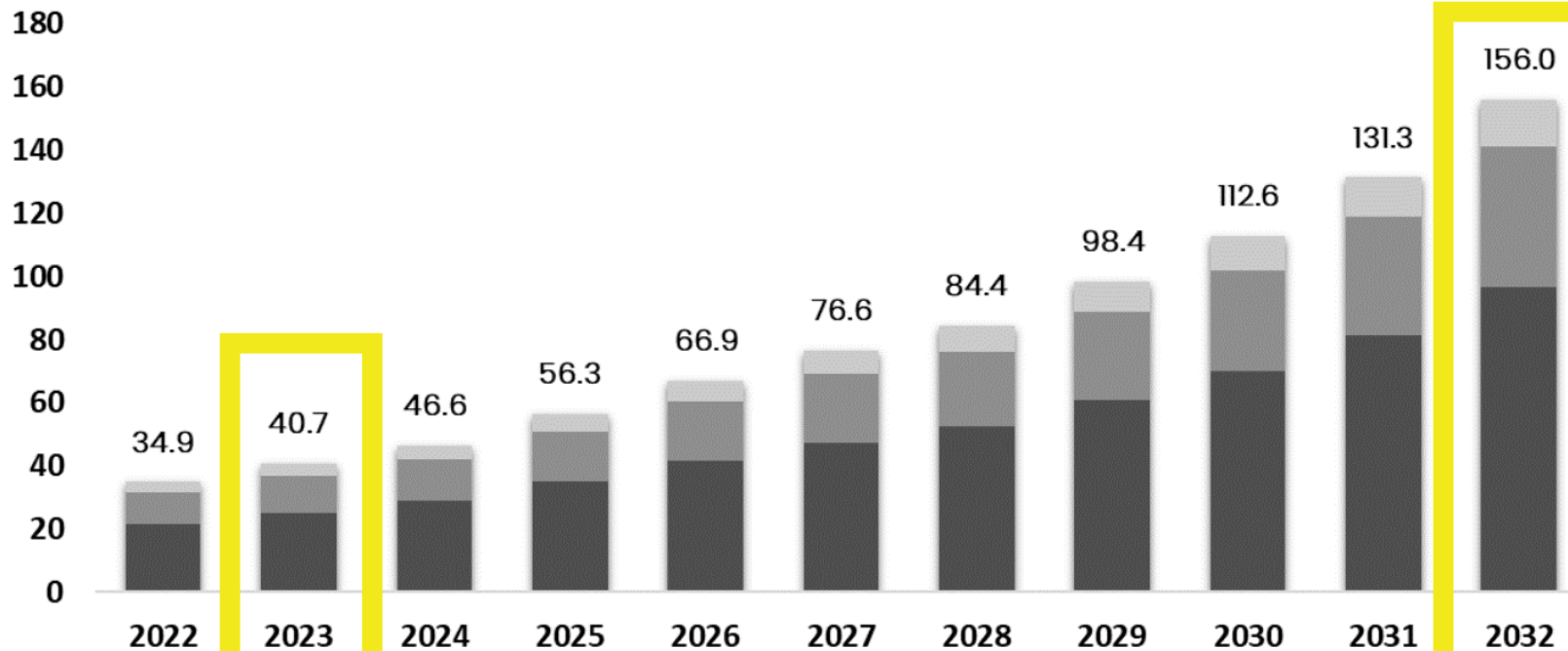


Tech Advances + Consumer Demand Fuels Rapid Growth

Global Wearable Medical Device Market

Size, by Product, 2022-2032 (USD Billion)

■ Diagnostic ■ Therapeutic ■ Patient Monitoring



The Market will Grow
At the CAGR of:

16.6%

The forecasted market
size for 2032 in USD:

\$156.0B

market.us
ONE STOP SHOP FOR THE REPORTS



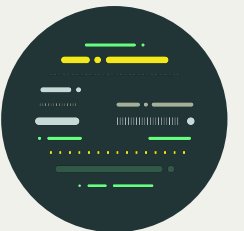
North America Outpaces the Rest of the World

Global Wearable Medical Device Market

Regional Analysis in 2022



North America is Expected to hold The Largest Global Wearable Medical Device Market Share



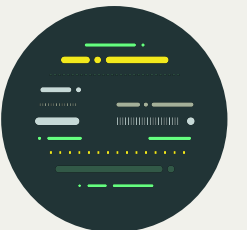
Overview of Applicable Fraud & Abuse Laws



Anti-Kickback Statute

(42 U.S.C. § 1320a-7b)

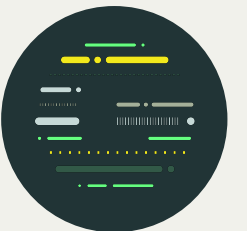
- Criminal law that prohibits the exchange of anything of value to induce or reward the referral or generation of Federal healthcare business.
 - Safe harbors offer protection from prosecution
- Purpose: Combat bribery and prevent undue influence on medical decision-making.
- Penalties:
 - Fines: Up to \$50,000 per kickback plus three times the amount of the remuneration
 - Exclusion: OIG is legally required to exclude convicted individuals or entities under 42 U.S.C. Sec. 1320a-7



False Claims Act

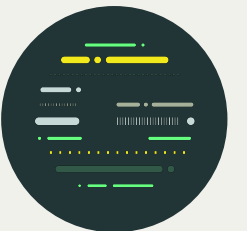
(31 U.S.C. § § 3729-3733)

- Violated when false claims for reimbursement are submitted to the government.
- Manufacturers are liable when they cause (i.e., induce) false claims by providing false or misleading information.
- **Purpose:** Combat fraud and protect the government from overpaying or paying for unnecessary goods/services
- **Penalties:**
 - Fines: \$11,181-\$22,363 per false claim plus three times the amount of the claim
 - Exclusion: OIG is legally required to exclude convicted individuals or entities under 42 U.S.C. Sec. 1320a-7



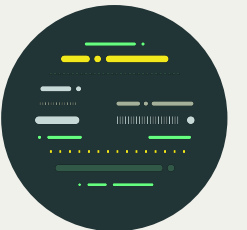
Physician Self-Referral Law (Stark Law) (42 U.S.C. § 1395nn)

- Prohibits physicians from referring patients to receive “designated health services” payable by Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship.
 - Financial relationship includes ownership/investment interests and compensation arrangement
 - Designated health services: laboratory services, physical therapy, radiology, DME and supplies, etc.
 - Strict liability statute (no proof of specific intent to violate is required)
- **Purpose:** Prevent undue influence on medical decision-making
- **Penalties:** Fines, exclusion



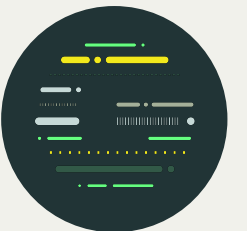
Beneficiary Inducement Civil Monetary Penalties (“CMP”) Law (42 U.S.C. § 1320a-7a(a)(5))

- Provides for the imposition of civil monetary penalties (fines) against any person who offers or transfers remuneration to a Medicare or state health program beneficiary that the person knows or should know is likely to influence beneficiary selection of a particular provider, practitioner, or supplier, for which payment may be made in whole or part by Medicare or State health care program.
 - Safe harbors offer protection from prosecution
- **Purpose:** punitive fines deter fraud, prevent recurrence
- **Penalties:** range from \$5,000 to \$100,000+ per violation, depending on the conduct involved

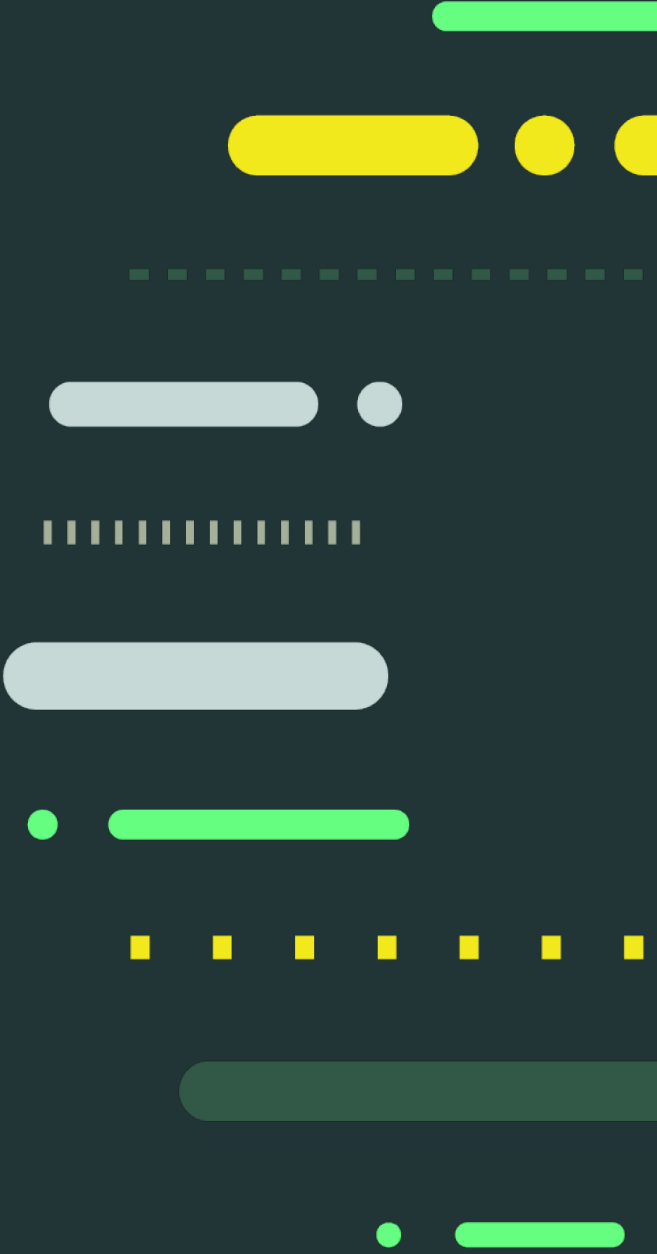


Corporate Practice of Medicine Doctrine

- Common law doctrine that prohibits corporations from practicing medicine or employing a physician to provide professional medical services.
 - 33 states have CPOM regulations/laws
 - Most states have exceptions for professional corporations
- **Purpose:**
 - Allowing corporations to practice medicine will result in the commercialization of the practice of medicine
 - Corporation's obligation to its investors/shareholders may not align with a physician's obligation to his patients
 - Employment of a physician by a corporation may interfere with the physician's independent medical judgment
- **Penalties:**
 - Depends on jurisdiction, includes criminal, civil penalties, license revocation, injunctions, exclusion, malpractice, product liability.

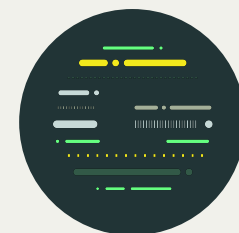


Compliance Considerations in High-Tech Healthcare



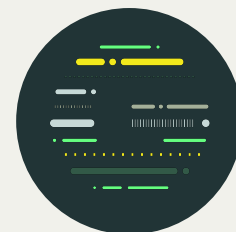
Payment and Reimbursement

- Payment structure
 - Self-pay vs. insurance coverage
 - Rental/loan arrangements
 - Capital + disposables (refills) costs
 - Patient inducement considerations?
- Is the company sharing appropriate reimbursement information?
- Is the company sharing truthful, accurate, and on-label coding/billing guidance?



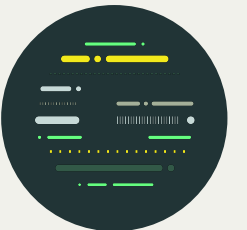
Provision of Products and Services

- Does the product provide a service or something of value to the HCP or institution?
- Remuneration to a patient that is likely to influence their selection of a provider, practitioner, or supplier?
- Is the company engaging in the corporate practice of medicine?
 - AI/ML considerations



Durable Medical Equipment (DME) Considerations

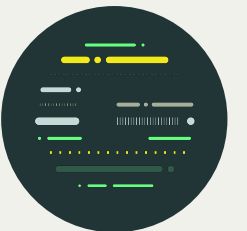
- Billing compliance
- DMEPOS Quality Standards
- CMS-approved accreditation organization
- Manufacturer vs. DME roles



Cybersecurity

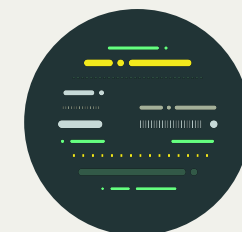
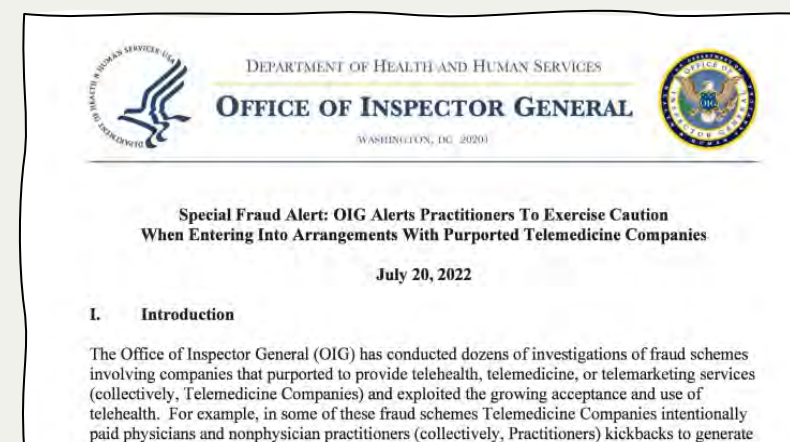
DOJ's Civil Cyber-Fraud Initiative

- Uses the False Claims Act to hold entities and individuals accountable for “deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.”
 - Press Release: Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (October 6, 2021)



Telemedicine

- Special Fraud Alert: OIG Alerts Practitioners To Exercise Caution When Entering Into Arrangements With Purported Telemedicine Companies (July 2022)
- DOJ is targeting telemedicine fraud schemes
- OIG's "Suspect characteristics":
 - Patient recruitment strategies
 - Lack of meaningful patient contact or information to assess medical necessity
 - Compensation based on the volume of orders/prescriptions
 - Either excludes Federal healthcare program beneficiaries or works solely with them
 - Company focuses on a single product or class of products (e.g., DME, genetic testing, prescription creams)
 - Lack of follow-up with patients



Clinical Laboratory Testing

- Heightened scrutiny for fraud and abuse
- Common types of fraud:
 - Unnecessary testing
 - Unauthorized testing
 - Unbundling tests
 - Kickbacks and bribes
 - Unlicensed testing
 - Tests by unqualified persons

PRESS RELEASE

Justice Department Charges Dozens for \$1.2 Billion in Health Care Fraud

Wednesday, July 20, 2022

Share >

For Immediate Release
Office of Public Affairs

Nationwide Coordinated Law Enforcement Action to Combat Telemedicine, Clinical Laboratory, and Durable Medical Equipment Fraud

The Department of Justice today announced criminal charges against 36 defendants in 13 federal districts across the United States for more than \$1.2 billion in alleged fraudulent telemedicine, cardiovascular and cancer genetic testing, and durable medical equipment (DME) schemes.

The nationwide coordinated law enforcement action includes criminal charges against a telemedicine company executive, owners and executives of clinical laboratories, durable medical equipment companies, marketing organizations, and medical professionals. In connection with the enforcement action, the department seized over \$8 million in cash, luxury vehicles, and other fraud proceeds.

Additionally, the Centers for Medicare & Medicaid Services (CMS), Center for Program Integrity (CPI) announced today that it took administrative actions against 52 providers involved in similar schemes.

“The Department of Justice is committed to prosecuting people who abuse our health care system and exploit telemedicine technologies in fraud and bribery schemes,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division. “This

TOP



Key Takeaways

- Implement a comprehensive compliance program that addresses legal, regulatory, and ethical considerations (e.g., ethical AI/ML)
- Stay informed
- Strong cross-functional collaboration between compliance/legal, IT, and medical
- Pay attention to risk areas:
 - Coding and billing
 - Ordering/prescribing process
 - Practicing medicine vs. aiding HCPs in making treatment and clinical decisions
 - "Follow the money," but also, is value being provided without payment in return?



Questions

Amanda Johnston
Managing Attorney
ajohnston@gardner.law
Phone: 763-639-6951



GARDNER
FDA LAW FIRM



fieldfisher

About Fieldfisher

9th November 2023

Dr Cord Willhoeft, LL.M.

About Fieldfisher

Fieldfisher is a European law firm with market-leading practices in many of the world's most dynamic sectors.



Key practice areas

- Energy and Natural Resources
- Financial Markets and Products
- Life Sciences & Healthcare
- Technology

Life Sciences & Healthcare

We provide comprehensive advice to companies in the MedTech industry on all legal issues such as placing devices legally on the Union market, interactions with healthcare professionals, product-related advertisement, pricing and reimbursement, data privacy, clinical trials and studies, distribution agreements, as well as corporate and HR. **Our team supports you along the entire life cycle and value chain in Life Sciences and Healthcare operations.**

Our Life Sciences Practice

Expertise	Regulatory	Market Access	Healthcare Compliance	Technology & Data	Corporate	Employment	Commercial Anti-trust
Area	Approval of medical devices	Pricing and Reimbursement	Interactions HCPs/HCOs	GDPR Compliance	Establishment of a GmbH	Employees in EU / Germany	Distribution Agreements with Customers
Tasks	<ul style="list-style-type: none"> MDR Compliance for Economic Operators MDR Conformity Assessments Marketability Legacy Devices Disputes with NBS 	<ul style="list-style-type: none"> Reimbursement under national Health Insurance Schemes E.g. Germany: DRG and NUB-Applications 	<ul style="list-style-type: none"> Drafting / Negotiating HCP Agreements Product-related Advertisement Code of Conduct Compliance Trainings 	<ul style="list-style-type: none"> Processing Patient / HR Data GDPR Compliance 	<ul style="list-style-type: none"> Founding Corporate Entity Transactions Corporate Secretarial Service 	<ul style="list-style-type: none"> Employment Contracts and Policies Litigations 	<ul style="list-style-type: none"> Distribution Agreements Terms & Conditions Competition law Review of Supply Models

Selection of our clients



Market feedback



► “Consistently excellent quality.”
— (Legal 500) 2023



► “Pragmatic and economical approach. Always committed, always available.”
— (JUVE Handbook) 2022/2023

Our European Life Sciences Team

fieldfisher



Dr Cord Willhöft, LL.M. (KCL)
Partner | Germany
cord.willhoeft@fieldfisher.com



Olivier Lantrès
Partner | France



Taly Dvorkis
Director | UK



Hector Jausas Farre
Partner | Spain



Marcel Willems
Partner | Netherlands



Oliver Süme
Partner | Germany



Elena Mitzman
Manager | Italy



Sarah Ellson
Partner | UK



Natalie Konings
Counsel | Belgium



Dr Thomas Rum
Partner | Austria

EU MedTech Healthcare Compliance Update

9th November 2023

Dr Cord Willhoeft, LL.M.

Your contact

fieldfisher



Dr Cord Willhoeft, LL.M.
Partner | Life Sciences Regulatory
Munich, Germany

+49 (0)89 62 03 06 245
cord.willhoeft@fieldfisher.com

- **EU Healthcare Compliance: Lack of a Legal Regime / Existing Industry Standards**
- **Product-related Advertisement for Medical Devices in the EU: Latest Trends**
- **Healthcare Compliance Updates:**
 - **Germany**
 - **The Netherlands**
 - **Italy**
 - **France**

EU Healthcare Compliance (1/2)

- **Legal Regime**
 - No “EU Law” for interactions with HCPs and HCOs
 - In theory: 27 Member States could mean 27country-specific set ups
 - No EU Sunshine Act (Transfer of Value), patchwork among the member states
- **Harmonized legal regime:**
 - EU Medical Device Regulation (EU MDR) since 26th May 2021
 - EU Directive 2001/83 for Medicinal Products, provides a fully harmonized legal framework for medicinal products (ECJ Judgement “Gintec C-374/05” on 8th November 2008)
 - GDPR



EU Healthcare Compliance (2/2)

- **However, principles for cooperation with HCPs / HCOs are the same:**
 - Principle of Transparency
 - Principle of Separation
 - Principle of Equivalence
 - Principle of Documentation
- **Useful reference / source for US legal departments:**
 - MedTech Europe Code of Ethical Business Practice (revised as of 1 January 2023), and
 - MedTech Europe Compliance Handbook (November 2022).



Overview of national rules on interactions with HCPs and HCOs and status of national transposition of the MedTech Europe Code of Ethical Business Practice

Compliance
Handbook

Product-related Advertisement in the EU (1/5)

New since 26 May 2021: MDR sets EU-wide applicable rules for the promotion of medical devices:

REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 5 April 2017

on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

Article 7

Claims

In the labelling, instructions for use, making available, putting into service and advertising of devices, it shall be prohibited to use text, names, trademarks, pictures and figurative or other signs that may mislead the user or the patient with regard to the device's intended purpose, safety and performance by:

- (a) ascribing functions and properties to the device which the device does not have;
- (b) creating a false impression regarding treatment or diagnosis, functions or properties which the device does not have;
- (c) failing to inform the user or the patient of a likely risk associated with the use of the device in line with its intended purpose;
- (d) suggesting uses for the device other than those stated to form part of the intended purpose for which the conformity assessment was carried out.



Product-related Advertisement in the EU (2/5)

- *“... it shall be prohibited to use text, names, trademarks, pictures and figurative or other signs that may mislead the user or the patient ... by:*
 - (a) ascribing functions and properties to the device which the device does not have;*
→ **misleading statements**
 - (b) creating a false impression regarding treatment or diagnosis, functions or properties which the device does not have;*
→ **misleading impressions**
 - (c) failing to inform the user or the patient of a likely risk associated with the use of the device in line with its intended purpose;*
→ **omit mandatory information**
 - (d) suggesting uses for the device other than those stated to form part of the intended purpose for which the conformity assessment was carried out.*
→ **suggesting of off-label use**



Product-related Advertisement in the EU (3/5)

- **EU Law (Art. 7 MDR)** allows product-related advertising for medical devices to the general public and HCPs
- **Germany** & the **UK** did not implement national prohibitions for the promotion of medical devices to lay persons / general public.
- However, there is a trend among the member states to further regulate product-related advertisement to patients:
 - French Medical Charta on the Promotion of Medical Devices
 - Polish Act on Medical Devices (DoA: 1 January 2023)



Product-related Advertisement in the EU (4/5)

Country	Advertising addressed to the General Public / Patients / Lay Persons
Austria	Advertisement of medical devices (i) available on prescription only, or (ii) only to be used by HCPs is prohibited.
Spain	Advertisement of medical devices (i) reimbursed by the national health insurance, or (ii) only to be used by HCPs is prohibited.
Poland	Advertisement of medical devices only to be used by HCPs is prohibited.
France	Advertisement of class IIb and III medical devices reimbursed by the national health insurance is prohibited. Advertisement of medical devices with a significant risk to human health need prior authorization by the French Drug Agency.
Italy	Advertisement of medical devices shall strictly follow an authorization procedure described by the Ministry of Health. <u>Exception:</u> No authorization procedure for medical devices like glasses and condoms and advertisements that call out the medical device individually or as a whole and include only the product name or the product's field.

Product-related Advertisement in the EU (5/5)

- Challenge: EU-wide accessible company websites!
- Risk Mitigation: Educational language & Disclaimer

“By clicking you are confirming that you are engaged in a health care profession. All information on this website henceforth is directed exclusively at health care professionals and is not intended for any laypersons. All content and material is intended for informational purposes only and cannot and should not be relied upon to diagnose or treat any medical condition.

Please be additionally informed that in some EU countries (for example France and Poland) medical device advertisement to general public is not permitted. Therefore, if you are accessing this website from one of the countries and you are not a healthcare professional, you need to exit this site immediately.”



Healthcare Compliance: Country Update Germany

Increasing standard for Hospitality (lunch / dinner)

- Providing lunches / dinners in context of internal educational events and working meetings is allowed within “reasonable limits”
- Since 2008: Meal limit of EUR 60-65; as of April 2023 upgrade to EUR 75
- Confirmed by official press release 25th May 2023, not included in BVMed Kodex (April 2023)

Country	Meal Limits
Germany	EUR 75
Spain	EUR 80
Italy	EUR 60
France	EUR 70 (prior CNOM approval required)
UK	ABHI: „reasonable“ / NHS: £75



Healthcare Compliance: Country Update The Netherlands

GMH published new “Indexation of maximum hourly rates for HCP services” (!):

Maximum hourly rates as of 1 January 2023

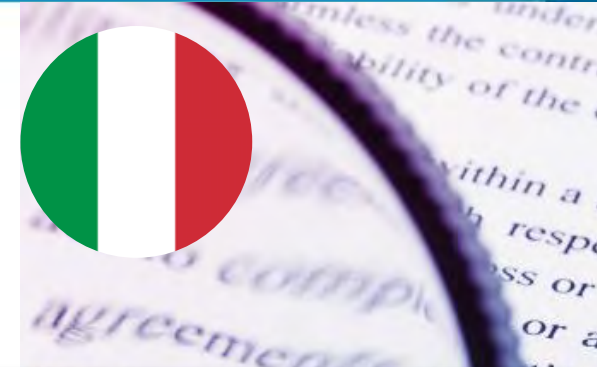
Category	Maximum hourly rate
Professor	EUR 267
University + further medical training > 3 years	EUR 187
University + further medical training ≤ 3 years	EUR 133
University: Masters degree without further medical training	EUR 113
HBO: Bachelors degree	EUR 100
Other	EUR 87

EU-wide unique approach, influence on other member states FMV?



Healthcare Compliance: Country Update Italy

- Italian Sunshine Act (31st May 2022): The Sun might shine in Italy soon...
- Implementation Decree and Draft Technical Specifications were published only August 2023 (public consultation ongoing), legal basis for digital Public Register.
- Final approval expected end of this year.
- Transfer of Value to be disclosed:
 - HCPs: Value > EUR 100 or annually > EUR 1,000
 - HCOs: Value > EUR 1000 or annually > EUR 2,500
 - Agreements with HCPs that create indirect benefit, such as participation in conferences, advisory boards, etc.
 - HCPs/HCOs that own company shares or IP rights



Country	Sunshine Law	MedTech Europe
Belgium	+	-
France	+	-
Germany	-	+
Italy	(+)	-
The Netherlands	+	-
Portugal	+	-
UK	-	+

Healthcare Compliance: Country Update France (1/2)

French Medical Charta for the Promotion of Medical Devices



Goal: regulate commercial, promotion, presentation or information practices which could adversely affect the quality of care or lead to unjustified expenditure by the health insurance system.

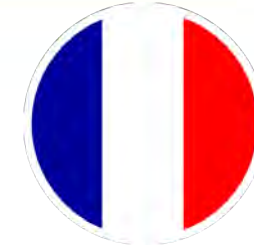
Timeline: Law published in March 2022 but mandatory registration planned for **Spring 2025**

The agency (CEPS) will be able to impose **financial sanctions** in case of non-compliance with the Charter.

- * Information provided to the beneficiaries must at least be a clear and accurate communication on all the associated regulatory and scientific aspects and mainly cover the mandatory information to provide regarding promotion of MDs
- * Experimental phase: threshold of 4 visits per year per company
- * No use of incentives

Healthcare Compliance: Country Update France (2/2)

Influencer Marketing and Medical Devices



- **France:** In June 2023 a new law was published which defines a new legal framework for how influencers can communicate on the social networks.
 - strict rules governing advertising and medicines or advertising and MD/IVD-MD, formally apply to influencers
 - influencer must clearly mention “Advertising” or “Commercial collaboration” along with the communication concerning the product

Spain	general guidelines called the Code of Conduct for the use of influencers.
Italy	specific guidelines issued by the Ministry of Health.
Germany / UK	Such a specific formal law does not exist in Germany or the UK

- If influencer marketing is seen as advertising in the sense of Art. 7 MDR, all requirements for advertising have to be met.
- It will be interesting to see how the self-regulatory market of the medical sector will handle influencer marketing in the future.

Questions?

9th November 2023

Dr Cord Willhoeft, LL.M.



Med-Tech Meets High-Tech

Privacy, Cybersecurity and AI in Connected Devices

Paul Rothermel

Thursday, November 9th, 2023

Presenter Introductions

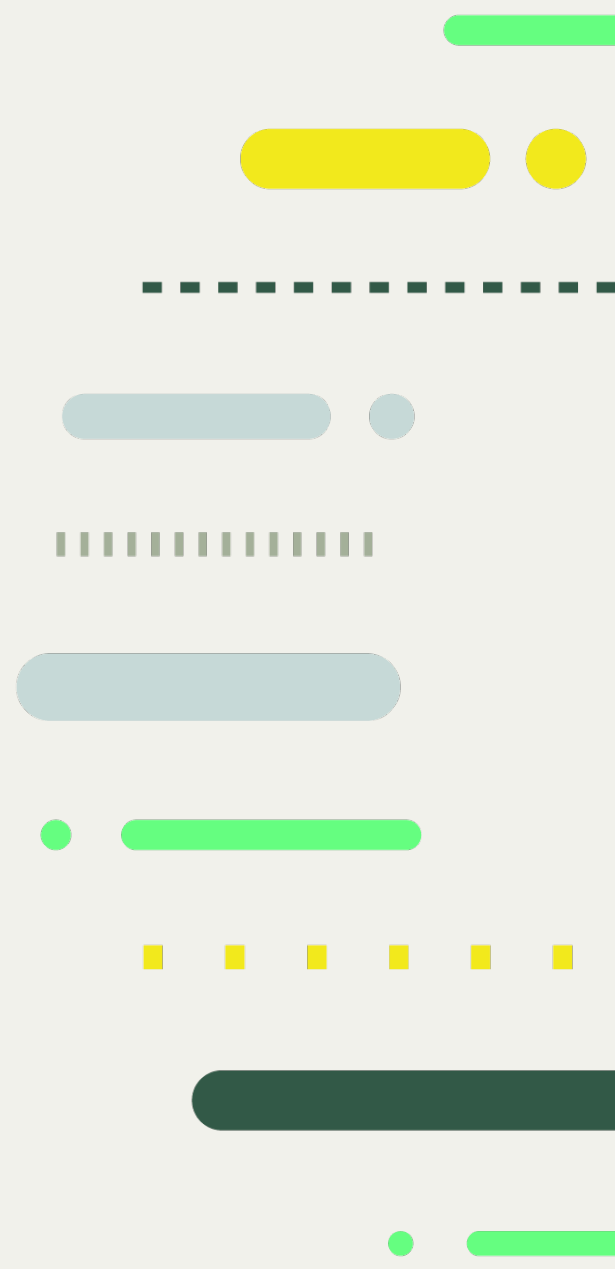


Paul Rothermel specializes in privacy and cybersecurity, including HIPAA, CCPA, GDPR, and other state and international laws as well as health care compliance matters. Before practicing at Gardner Law, Paul worked in privacy and data protection at Medtronic, Inc. advising on privacy requirements for various areas including innovative health care technologies, clinical research, and vendor management. Before that, Paul was an attorney for the State of Minnesota, where he counseled on state and federal laws, including HIPAA implementation.

Paul Rothermel, J.D., CIPM

Senior Attorney
Prothermel@gardner.law
Phone: 651-364-7514

GARDNER
FDA LAW FIRM

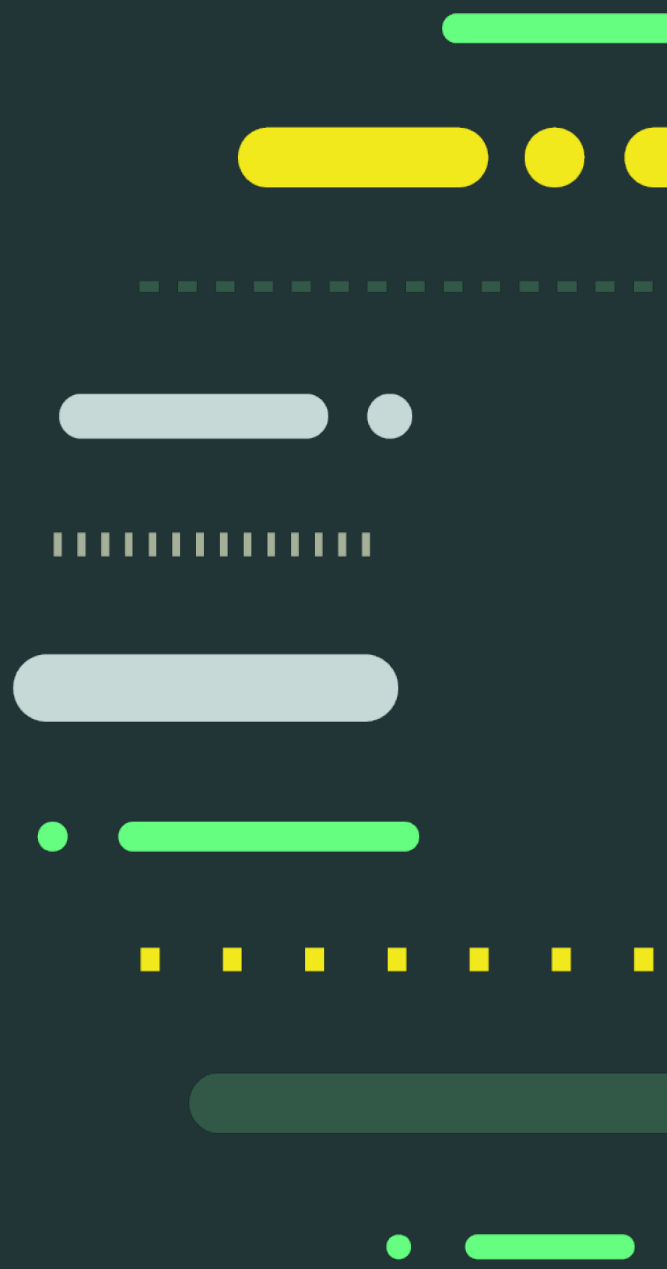


Agenda

- Background
- Laws and regulations
- Key considerations
- Conclusion
- Questions



Background



In the News

Safeguarding IoMT and connected devices is an ongoing challenge

Despite difficulties with in-depth scans and legacy software risks, the director of medical device and IoT security at Henry Ford Health says more responsibility from device manufacturers and new regs from the FDA make him optimistic.


By [Mike Miliard](#) | August 30, 2023 | 11:00 AM

Medical Practices with a High Percentage of Connected Medical Devices Experience More Cyberattacks

Posted By Steve Alder on Dec 6, 2022

US regulator takes action to ensure internet security in connected medical devices

HEALTH - FDA Mandates Internet Vulnerability Check for Medical Devices with Internet Access

NEWS 2 APRIL 2023 

Data privacy concerns hamper adoption, use of personal medical devices

While Americans think consumer tech is driving more connected relationships with their providers, they also see voice technology and AI with a skeptical eye.

By [Nathan Eddy](#) | January 08, 2020 | 11:04 AM

Weak Connected Medical Device Security Increases Cyberattack Threats

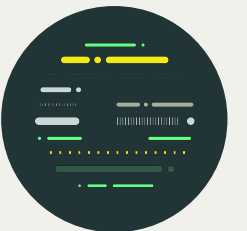
A new survey found that healthcare organizations with more connected medical devices have a 24 percent greater risk for cyberattacks, underscoring a need for more medical device security.

 By [Sarai Rodriguez](#)



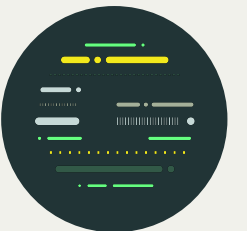
Many Types of Connected Devices

- At-home
 - Durable medical equipment (DME)
 - Patient monitoring/wearables
 - Implants
- In-clinic
 - Blood pressure monitors, oximeters, medical imaging, etc.
- Software (“SaMD”)
- And more

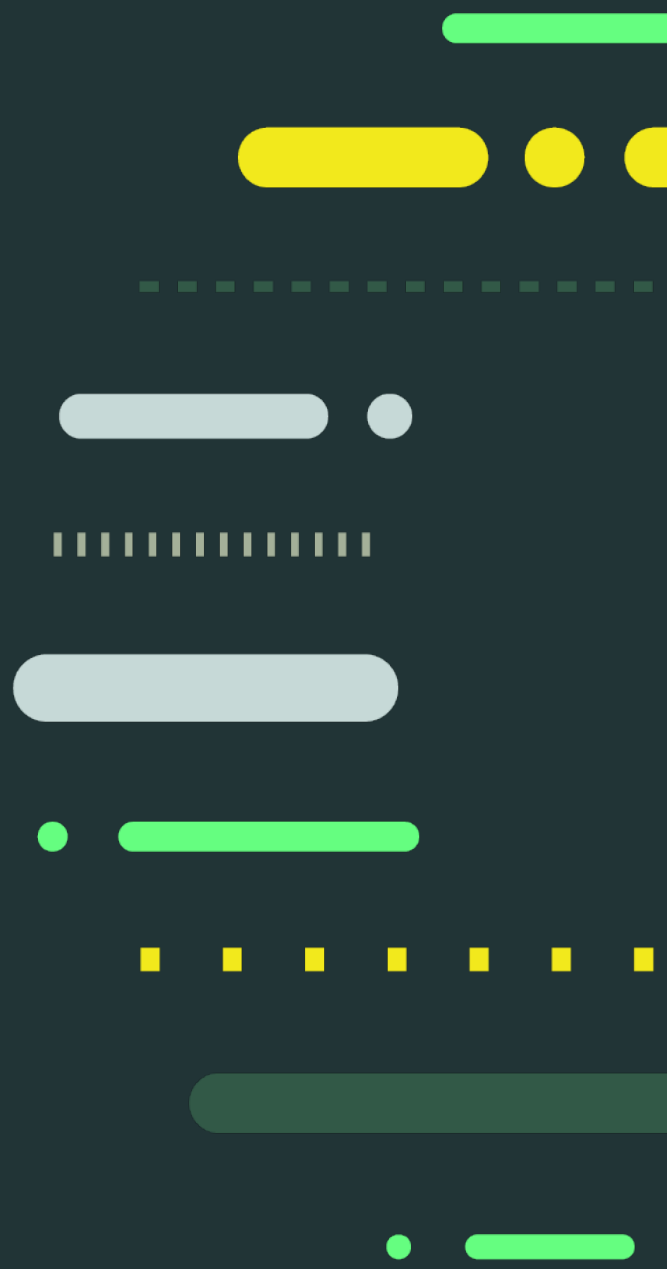


Many Variables

- Business model
 - Contractual relationships
 - Servicing of devices/equipment
 - Software and/or physical products
- Device type
 - Data collection
 - Clinical trial vs. commercial
- Direct-to-patient relationship (e.g., DME)
- Data use
 - R&D, research, marketing, other
 - AI/ML
- Data ownership

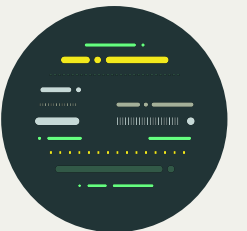


Laws and Regulations



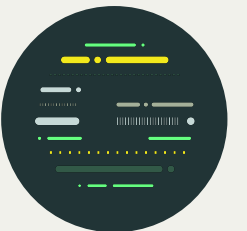
Laws and Regulations

- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Federal Trade Commission Act (“FTCA”)
- State laws (California, Washington, etc.)
- Food, Drug, and Cosmetic Act (“FDCA”)



HIPAA

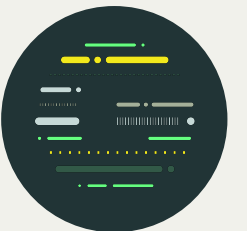
- Applies to Covered Entities and Business Associates
 - Governs use and disclosure of Protected Health Information (“PHI”)
- Applies to some manufacturers, including:
 - DME manufacturers (typically Covered Entities)
 - Certain connected device makers (often Business Associates)
 - Other activities (e.g., reimbursement support)
- Restricts disclosure AND use of PHI
- Limits use of PHI by business associates (even de-identification)
- Security safeguards



FTCA

- Regulates consumer protection generally
- “Unfair and deceptive trade practices” violate Section 5 of FTCA*
- FTC is focused on consumer harms including:
 - Lax data security
 - Misuse of biometric and personal data
 - Failure to live up to promises (including implied commitments)
 - Consent that is unclear, vague, or misleading
- Regarding AI, FTC has also expressed interest in:
 - Misuse of data
 - Copyright/IP
 - Bias and inaccuracy
 - Limited pathways for appeals

*See 15 U.S.C. Sec. 45(a)(1)



State Privacy Laws

- Explicit consent to process consumer health data
- Geofencing restrictions
- Data security
- Opt-outs
- Data protection assessments
- Processing agreements
- Breach notification requirements



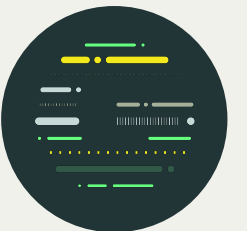
Federal FD&C Act

- Quality system regulations (QSR)
- Food & Drug Administration (“FDA”) guidance on cybersecurity

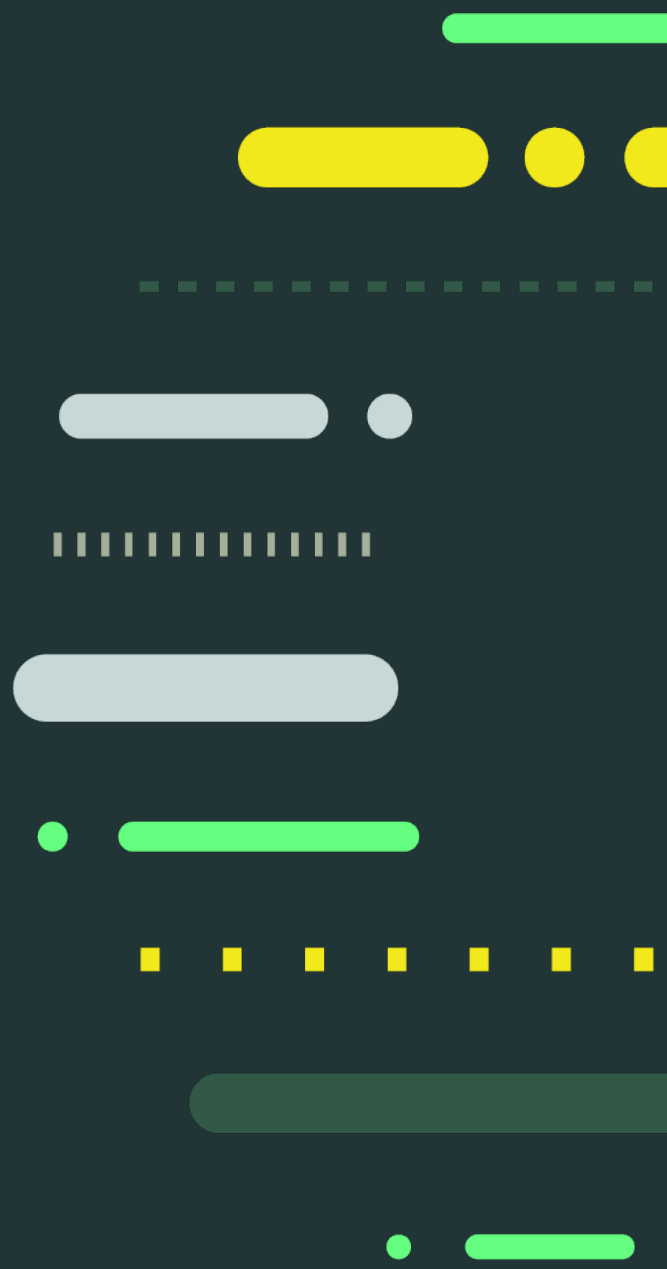
Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.



Key Considerations



General Considerations

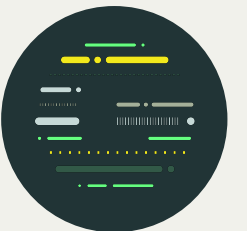
```
...mod.use_x = True
...mod.use_y = False
...mod.use_z = False
...eration == "MIRROR"
...mod.use_x = False
...mod.use_y = True
...mod.use_z = False
...eration == "MIRROR"
...mod.use_x = False
...mod.use_y = False
...mod.use_z = True
...ction at the end
...b.select= 1
...ob.select=1
...xt.scene.objects.a
...lected" + str(modi
...or_ob.select = 0
...y.Context.selected
...objects[one.name]
...("please select ex
...OPERATOR CLASSES
...es.Operator):
...X mirror to the sel
...ect.mirror_mirror_
...or X"
...text):
...t.active_object is
```

1. Do cybersecurity
2. Document data flow
3. Understand data collection
4. Anticipate data use/sharing
5. Consider patient rights
6. Plan contract provisions



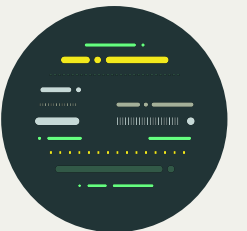
Durable Medical Equipment

- HIPAA Privacy and Security Rules
- Patient agreements and consent
- Data sharing with prescribers (treatment vs. business associate)
- Third-party risk (vendors, cloud providers)
- Business associate/data protection agreements
- FDA cybersecurity guidance
- Data ownership/IP



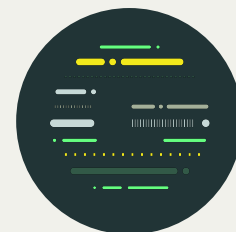
Remote Patient Monitoring

- Data minimization
- Who is data shared with (caregivers, HCPs?)
- Patient consent management (i.e., for sharing and withdrawal of consent)
- Business associate/data protection agreements
 - Data ownership
 - De-identification
 - Liabilities
 - Security requirements
- Third-party vendor risk
- Location tracking/geofencing regulations
- Biometrics regulation
- Manufacturer data collection/use



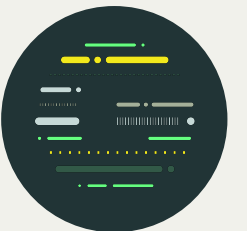
Implants

- Security of implant connectivity with programmers (including data security)
- Company access to PHI (servicing programmers, OR support, etc.)
- Cloud-connected vs. customer network-only
- Security requirements of customer (e.g., for laptop or tablet used to setup device)
- Manufacturer data collection/use
- Business associate/data protection agreements
- Third-party vendor risk



In-Clinic/Software

- Customer security requirements
- Servicing arrangements
- Access to PHI
- Cloud-connected vs. customer network only
- Business associate agreements
- Third party vendor risks
- Manufacturer data collection/use



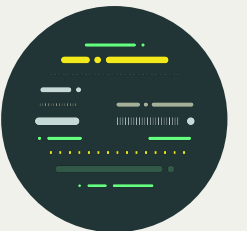
Clinical Trials

- Business associate agreements
- Sponsor vs. business associate role
- Many state privacy laws make exception for clinical research conducted in accordance with FDA or Common Rule requirements
- Address unique data flow and collection models in informed consent process

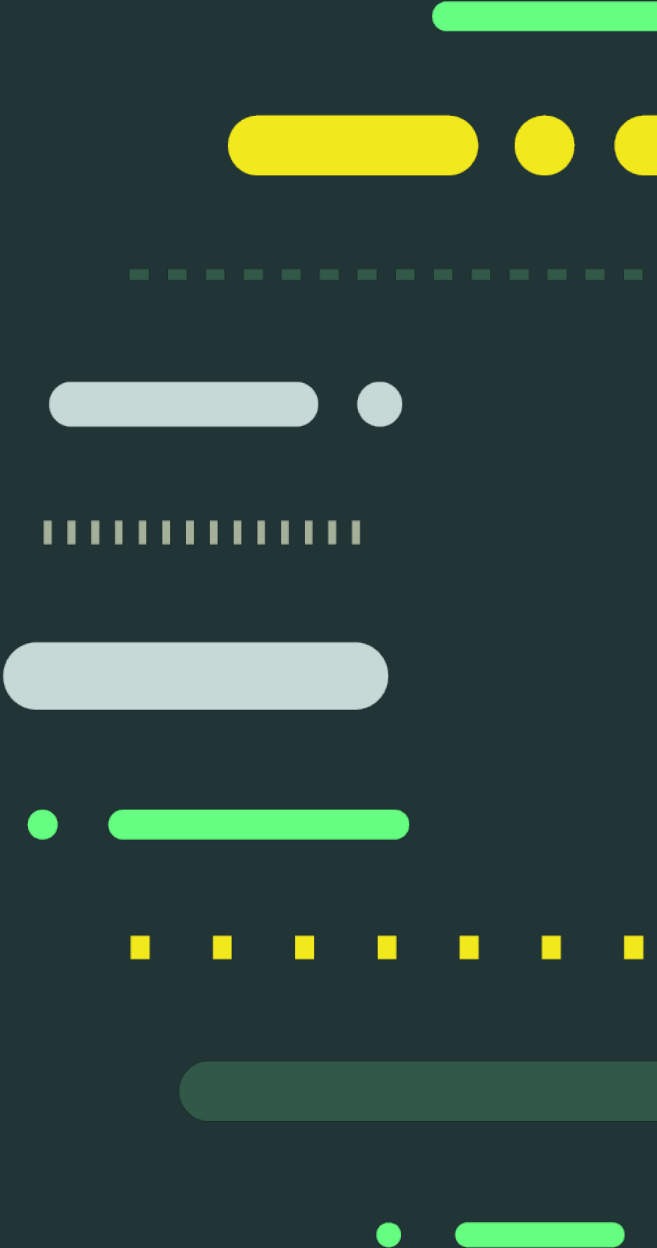


FDA Requirements: Safety and Effectiveness

- Follow applicable FDA and regulatory guidance on cybersecurity
- Consult with regulatory experts early to address submission requirements and plan for post-market cybersecurity requirements

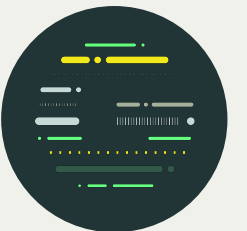


Conclusion

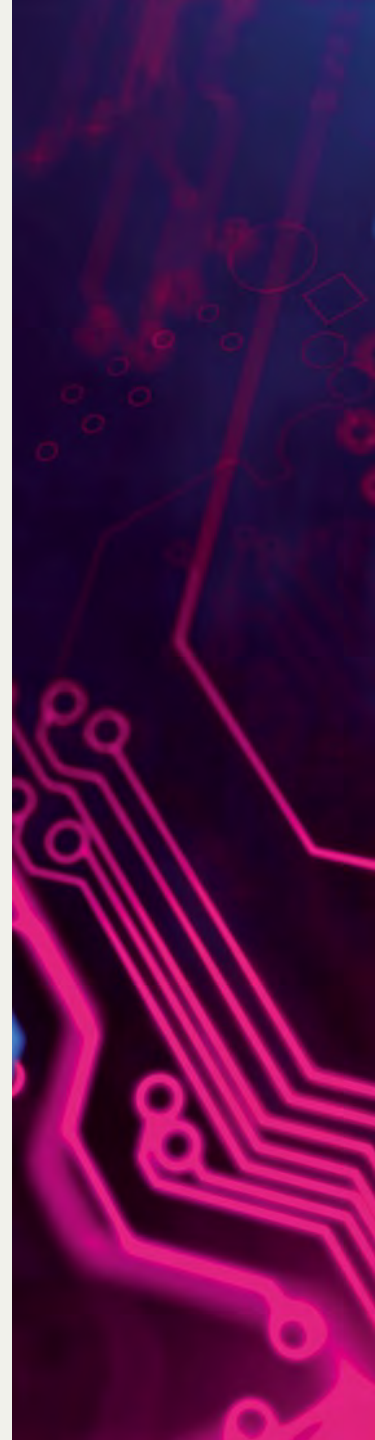


Key Takeaways

- Understand the data flow (how data will be collected, used, and shared)
- Plan contracts for company goals
- Determine patient consent requirements and approach
- Cybersecurity measures must address safety, effectiveness AND privacy of device/ecosystem
- Be flexible



EU and US Developments in AI



Questions

Paul Rothermel
Senior Attorney
prothermel@gardner.law
Phone: 651-364-7514



GARDNER
FDA LAW FIRM

Managing Privacy and Cybersecurity Risks in Connected Devices

9 November 2023

Oliver Sueme

Your contact

fieldfisher



Oliver Süme

Partner | Technology & Data
Hamburg, Germany

+49 40 87 88 698 537

oliver.sueme@fieldfisher.com

- **The European digital health market and security risks in the EU**
- **The “NIS2 Directive” and its impact for the Health industry**



The European digital health market and security risks in the EU

The European digital health market

- EU digital health market was valued at 21 billion Euro in 2019 and is expected to grow at an annual growth rate of 13.9% from 2020 to 2027, reaching €55.4 billion by 2027.
- The number of connected health devices in Europe increased from 500 million in 2018 to 620 million in 2019, and is projected to reach 1.4 billion by 2024.
- Main categories of connected health devices are
 - wearable devices
 - home health devices
 - clinical-grade devices (e.g. electrocardiograms (ECGs), pulse oximeters, and thermometers used by HCP's)
 - implantable devices (e.g. pacemakers, defibrillators, and insulin pumps)



Data Privacy and Security risks in the EU

- Connected devices in life sciences and the health sector, such as medical devices, health technology, and health services, are increasingly exposed to privacy and cybersecurity risks in Europe.
- Risks include data breaches, ransomware attacks, denial-of-service attacks, and cyber espionage, which can compromise the confidentiality, integrity, and availability of sensitive personal and health data, as well as the safety and performance of critical medical equipment and infrastructure.
- According to the statistics from the European Union Agency for Cybersecurity (ENISA), the number of reported cybersecurity incidents in the health sector increased by 47% between 2018 and 2019.
- Most common types of incidents were
 - system failures (40%)
 - malicious actions (37%)
 - human errors (23%).

The average duration of the incidents was 36 hours, and the average impact was 14,000 affected users

- The most affected services were emergency services, primary care, and hospital services



The “NIS2 Directive” and its impact for the Health industry

The EU's answer: The “NIS2 Directive”

- To address these challenges, the EU has adopted the NIS 2 Directive (*Directive EU 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union*)
- NIS2 replaces the previous *Network and Information Systems (NIS) Directive*
- Aims to establish a high common level of cybersecurity across the European Union and expands the scope of the sectors covered by the cybersecurity obligations, including a broader range of entities in the healthcare sector and manufacturers of certain medical devices.



NIS2 Directive

OVERVIEW

- Replaces and builds on previous NIS Directive
- **Background:** increased threats to network and information systems
- **Objective:** Increase cyber resilience and incident response capacities of public and private sectors

WHEN WILL NIS 2 APPLY?

- **Entry into force:** 16 January 2023
- Implementation into Member state law by **17 October 2024**

RELATIONSHIP WITH OTHER LEGAL INSTRUMENTS

- Horizontal cybersecurity law
- Supplemented by sector-specific laws

Scope and key concepts

1

Provide their services/ carry out their activities in the EU

2

Operate in one of the sectors listed in Annexes

Annex 1: Sectors of High Criticality
Annex 2: Other Critical sectors

3

Annex 1 (Excerpt)

Type of entity

- Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ⁽¹⁸⁾
- EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ⁽¹⁹⁾
- Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ⁽²⁰⁾
- Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2
- Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ⁽²¹⁾

- (a) Manufacture of medical devices and *in vitro* diagnostic medical devices
- Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council ⁽⁴⁾, and entities manufacturing *in vitro* diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council ⁽⁵⁾ with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive

Scope for the Health industry

- Scope of NIS 2 has been broadened to cover a wider range of healthcare entities, including manufacturers of medical devices, in vitro diagnostic medical devices and medical devices considered to be critical during a public health emergency.
- Such medical devices include wearable devices (fitness trackers, blood glucose trackers, etc.), telehealth solutions, in silico medicine, software as a medical device and digital twins, among others.
- Healthcare providers and entities that fall within the healthcare related subsectors must determine whether they are likely to be deemed "important" or "essential". This distinction is significant, as different requirements attach to each category.



Applicable Member State Law

- **Principle:** law of establishment
- **Exceptions:**
 - Providers of public electronic communications networks or providers of publicly available electronic communications services: place where services are provided
 - Public administration entities: jurisdiction of member state that established them
 - Cross-border services: staged approach



The Top 5 key changes under the NIS 2 Directive

1. Details **cyber risk management measures** that all covered organisations are required to put in place
2. Imposes **direct obligations on management** in respect of an organisation's compliance with the NIS 2 Directive, and **onerous penalties** where those are not complied with
3. Acknowledges the importance of **security** at all levels **in supply chains and supplier relationships**
4. Clarifies and strengthens **incident reporting requirements**
5. Provides **supervisory authorities greater supervisory powers and increases sanctions for non-compliance**



1. Expanded cybersecurity risk management measures

All organizations must take **appropriate and proportionate** technical, operational and organisational measures to:

- Manage risks to NIS used for operations or provision of services
- Prevent or minimise impact of incidents on recipients of services and on other services

“Appropriate” based on:

- State-of-the art + relevant EU and International standards;
- Cost of implementation

“Proportionate” based on:

- Degree of risk exposure
- Entity’s size
- Likelihood of occurrence
- Severity (societal and economic impact)

2. Management responsibility under NIS2

OBLIGATIONS

Management bodies must:

- **Explicitly approve and oversee** implementation of risk management measures
- Undertake cybersecurity training

SANCTIONS

Non-compliance of the organization may result in:

- **Personal liability** for management
- Temporary prohibition to exercise managerial functions (essential entities only)

3. Supply chain security diligence

Security due diligence of direct suppliers or service providers to assess and take into account:

- Vulnerabilities specific to each direct supplier and service provider
- Overall quality of products and cybersecurity practices (incl. secure development procedures) of suppliers and service providers
- Results from “coordinated security risk assessments”



Incorporation cybersecurity risk-management measures into contractual arrangements with direct suppliers and service providers (with potential back-to-back coverage).

4. Incident reporting

Reporting of significant incidents

Incident: event compromising availability, authenticity, integrity or confidentiality of data or the services

Significant:

- severe operational disruption of the services or financial loss for the entity
- or
- causing considerable material or non-material damage to other natural or legal persons

Early warning

- Within 24 hours after becoming aware
- Initial report with basic information (e.g. accidental/ malicious intent; likelihood cross-border impact)

Incident notification

- Within 72 hours after becoming aware
- Update of initial report: initial assessment of incident (severity, impact and indicators of compromise)

Final report

- Within one month after incident notification (!)
- Detailed description of incident, root cause, mitigation measures, cross-border impact (where applicable)

5. Supervision and sanctions

	Essential entities	Important entities
Supervision	<ul style="list-style-type: none"> • On-site inspections and off-site supervision • Regular and targeted security audits • Ad Hoc audits • Ex-post audits 	<ul style="list-style-type: none"> • Ex-post audits
Administrative sanctions	<ul style="list-style-type: none"> • Warnings and (elaborate) binding instructions • Cease and desist order • Order to take appropriate and proportionate TOM's • Order to inform users of cyber threat • Order to communicate publically about NIS 2 infringement • Order to implement recommendations of security audit • Suspension of authentication or certification • Temporary prohibition to exercise managerial functions at C-level/ rep level + personal liability 	<ul style="list-style-type: none"> • Warnings and (limited) binding instructions • Cease and desist order • Order to take appropriate and proportionate TOM's • Order to inform users of cyber threat • Order to communicate publically about NIS 2 infringement • Order to implement recommendations of security audit
Administrative fines	Higher amount of € 10 million or 2% of total worldwide annual turnover	Higher amount of € 7 million or 1,4% of total worldwide annual turnover

Key steps for organizations to ensure compliance



Identify whether your organization is caught

Map out the requirements that will apply to your organization

Conduct an audit of your existing processes to identify the gaps that will need to be plugged

Review contractual arrangements with your supply chain

Budget for the time and financial costs of implementing necessary changes

Train, train train!



fieldfisher

Questions?

9th November 2023

Oliver Sueme



Artificial Intelligence: Engaging FDA

Nathan Downing

Thursday, November 9th, 2023

Presenter Introduction



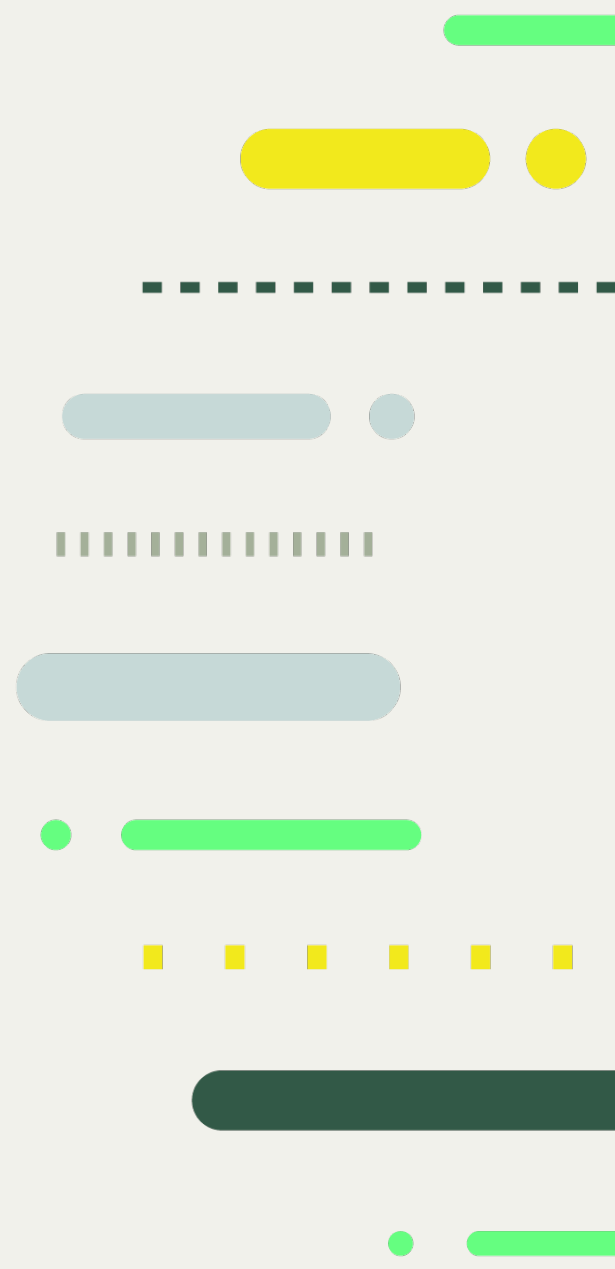
Nathan Downing, J.D.

Senior Attorney
ndowning@gardner.law
Phone: 651.353.6283

GARDNER
FDA LAW FIRM

Nathan focuses his practice on FDA-regulated clients. His industry experience allows him to provide actionable legal advice on a variety of health law matters.

Nathan regularly advises FDA-regulated clients on regulatory and compliance matters. He advises clients on their advertising and promotion programs, represents clients in front of the FDA on a variety of matters, and assesses industry initiatives for compliance concerns. Nathan's extensive regulatory experience allows him to advise clients regarding a variety of medical products, including pharmaceuticals, medical devices, medical foods, and nutritional supplements.



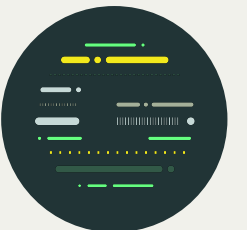
Agenda

- Introduction
- Artificial Intelligence
 - Medical Products
 - Medical Devices
- Regulations and Classifications
- Communication Strategies and Considerations
- Post-Market Considerations



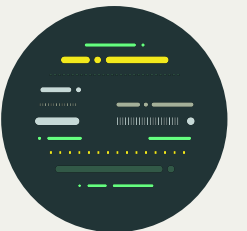
Artificial Intelligence in Medical Products

- FDA review of Artificial Intelligence/Machine Learning (AI/ML)-Enabled medical devices
 - Between 8/1/22 and 7/30/23, FDA added 155 AI/ML devices to its tracking list
 - FDA expects an approximate 30% year-over-year increase between 2022 and 2023
 - FDA has seen double-digit growth in this area yearly
- FDA also focusing on artificial intelligence in pharmaceutical manufacturing
 - Workshop held September 26-27, 2023
 - FDA published a discussion paper, which remains open for comment through the 27th of this month



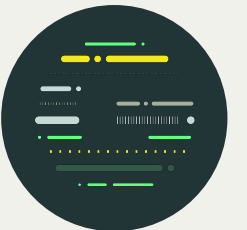
Artificial Intelligence/Machine Learning in Medical Devices

- Focus today is on strategy for approaching FDA with AI/ML medical device
- Consider the following:
 - Is your medical product a medical device regulated by FDA?
 - Does your device utilize AI/ML?
 - How is your device classified and what are potential paths for clearance/approval?
 - When and how will you utilize the pre-submission process?
 - What will be your change control strategy?



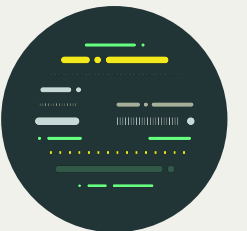
Understanding Your Medical Product

- When is it *truly* not a medical device?
- Medical device (where FDA exercises enforcement discretion)
- Medical device (or combination product)



AI/ML Part of the Regulated Product

- FDA defines artificial intelligence as using algorithms or models to perform tasks and exhibit behaviors such as learning, making decisions, and making predictions
- Machine learning is defined by FDA as subset of AI that allows models to be developed by training algorithms through analysis of data, without models being explicitly programmed
- If you have AI/ML in your product, confirm whether it is part of the regulated portion of the device
- Consider whether the AI/ML portion interacts with non-medical device components



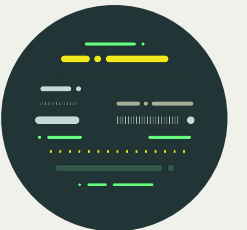
AI/ML Device Classifications and Corresponding Considerations

- General Classifications
- Class I/II Exempt
- Class II
 - Predicate
 - De novo
- Class III
 - Established testing pathway



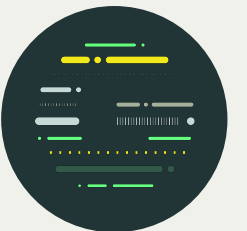
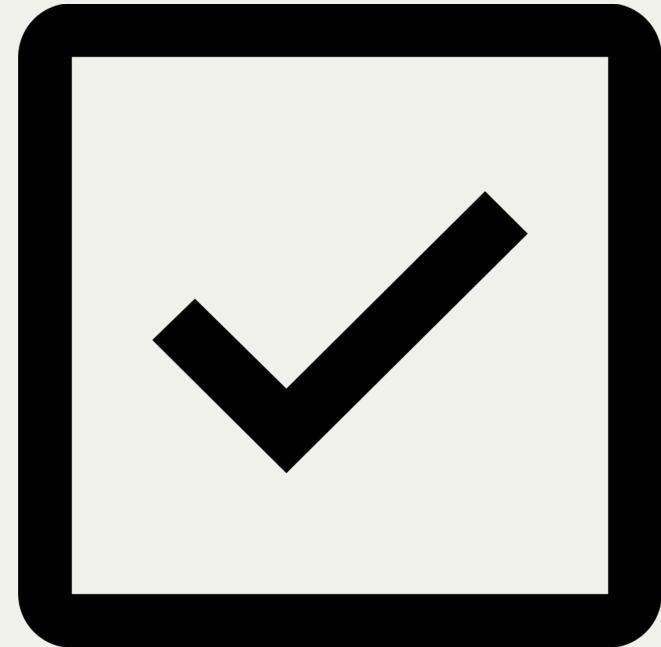
FDA Communication Strategy

- Pre-submission options
- Informational pre-submission
 - Option to start dialogue early
 - FDA will be in “listening mode”
- Pre-submission to clarify issues
 - IDE
 - Pre-market submissions
- Other opportunities
 - Requests for designation
 - 513(g)
 - Administrative Questions
 - Ongoing discussing during submission review



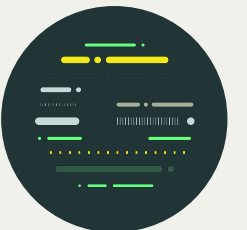
FDA Communication Considerations

- Be honest (obviously)
- Know what you know ... and what you don't
- Be on the same page with your team
- Take advantage of every opportunity
- Do not fear FDA



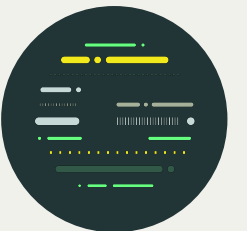
Post-Market Considerations

- Change Control
 - Frequency of changes
 - 510(k) devices
 - PMA devices



Conclusions

- FDA is familiar with AI/ML medical products, field is constantly changing
- Know your device
- Craft a communication strategy for FDA
- Take advantage of opportunities--be a PARTNER



Questions

Nathan Downing
Senior Attorney
ndowning@gardner.law
Phone: 651.353.6283



GARDNER
FDA LAW FIRM

Regulatory Update EU, Switzerland and UK

9th November 2023

Dr Cord Willhoeft, LL.M.

Your contact

fieldfisher



Dr Cord Willhoeft, LL.M.
Partner | Life Sciences Regulatory
Munich, Germany

+49 (0)89 62 03 06 245
cord.willhoeft@fieldfisher.com

- **EU Medical Device Regulation (EU MDR) / Amendment March 2023:**
 - **(Initial) MDR Transitional Periods and Impact on Supply Situation**
 - **MDR Amendment as of 20 March 2023**
- **Update Switzerland: Amendment of Swiss MedO (1 November 2023)**
- **Update UK: Acceptance of CE-marks (post-Brexit; April 2023)**
- **Software as Medical Device (SaMD) and Artificial Intelligence (AI)**

EU MDR Amendment (1/4)

REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 5 April 2017
on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and
Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
(Text with EEA relevance)

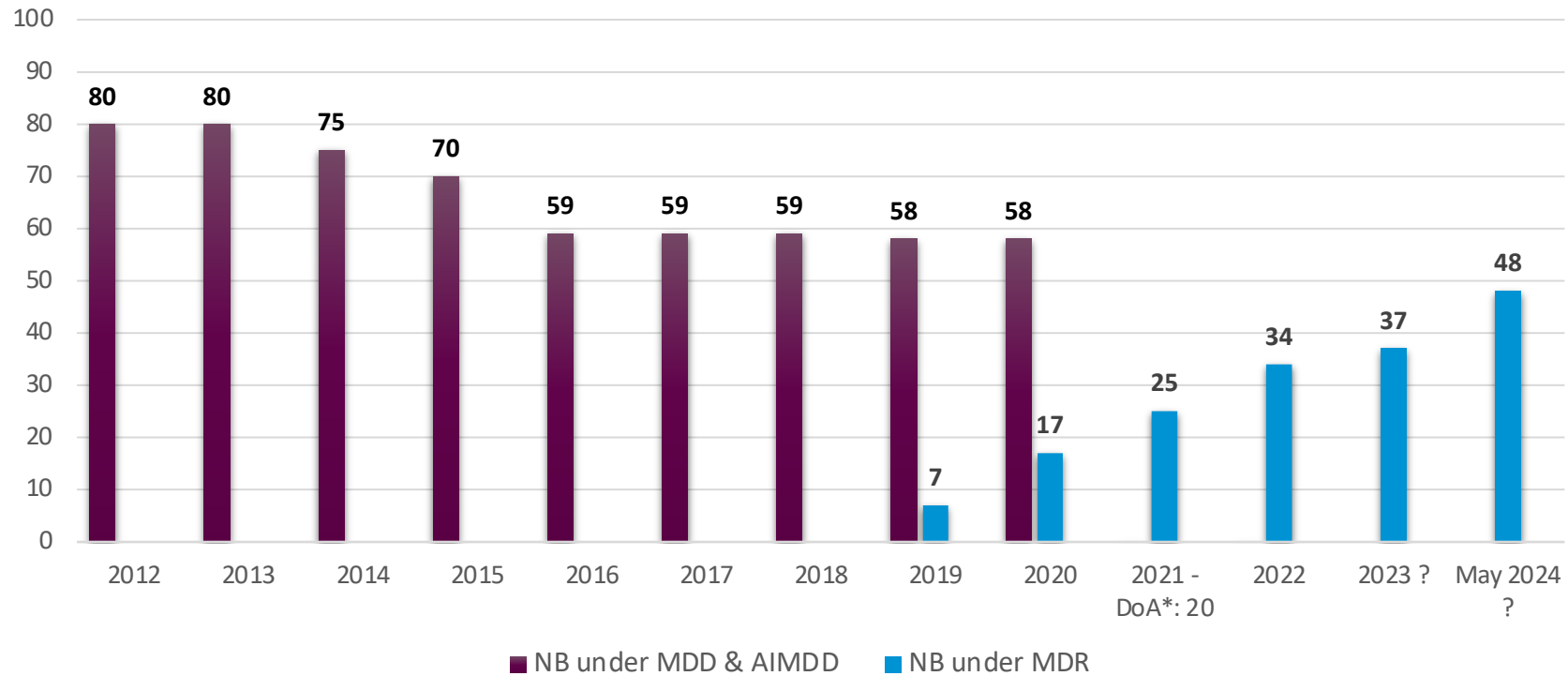


- **Regulation (EU) 2017/745 of 5th April 2017 on Medical Devices (“EU MDR”):**
 - Date of Application 26th May 2021 (IVDR 26th May 2022)
 - Directly applicable in all member states (EU Directive vs. Regulation)
 - Hugely extends regulatory framework medical devices on the Union market (MDD included 17 Articles 10 Annexes / EU MDR 127 Articles 17 Annexes)
- **(Initial) Transitional Periods:**
 - Notifications of Notified Bodies becomes invalid 26th May 2023
 - Legacy Devices may be placed on the Union market until MDD-certificate expires, but until 26th May 2024 the latest

EU MDR Amendment (2/4)

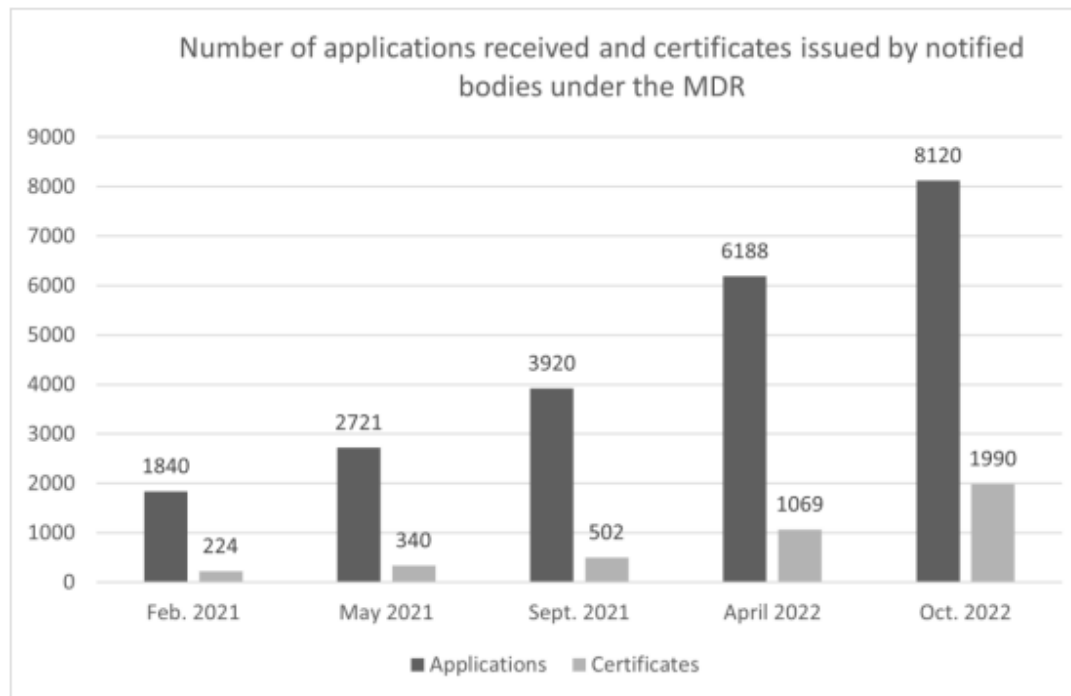
Number of Notified Bodies in the EU

Notification in Europe takes too long
- average duration of procedures since DoA: 700 days!



EU MDR Amendment (3/4)

- **21,376 MDD / AIMDD certificates that will expire until 26 May 2024 (2023/0005 [COD])**



- **Commission (6th January 2023):** *“This may cause shortages of medical devices, putting patient safety at risk.”*



EU MDR Amendment (4/4)

- **EU MDR (DoA 26 May 2021) Amendment as of 20 March 2023:**
 - Extension of the MDR Transitional Period for “Legacy Devices”
 - class I, IIa and IIb devices until 31 December 2028
 - class III and IIb implantable devices until 31 December 2027if certain requirements are fulfilled (e.g. manufacturer applied at NB for MDR conformity assessment procedure before 20 March 2023)
 - Removal of the “sell-off” period (26 May 2025) for devices already placed on the Union market
- **Applies only to so called legacy devices**, i.e. devices covered by a valid EC certificate issued in accordance with AIMDD or the MDD prior to 26 May 2021



Update Switzerland: Amendment of Swiss MedDO (1st November)

- **Background: Commission and Swiss Confederation were not able to update the existing MRA** (Medical Device Chapter, 2002), since MDR DoA
- **Temporary Solution:** Swiss Medical Device Ordinance refers to EU MDR, in relation to EU/CH-AR, placing on the market, CE-marks, etc., in order to secure marketability of CE-marked devices in Switzerland
- **Amendment of Swiss MedDO with effect of 1st November 2023**, to allow application of new transitional periods of the EU MDR also in Switzerland, i.e. marketability of
 - class I, IIa and IIb devices until 31 December 2028, and
 - class III and IIb implantable devices until 31 December 2027if certain requirements are fulfilled (e.g. manufacturer applied at NB for MDR conformity assessment procedure before 20 March 2023)



Update UK: Acceptance of CE-marks (post-Brexit)

- Introduction of the UKCA mark as the UK's post-Brexit replacement for the EU CE mark
- Government has put in place legislation that amends the Medical Device Regulations 2002 (SI 2002 No 618, as amended) (UK MDR) to extend the acceptance of CE marked medical devices on the Great Britain market:
 - general medical devices compliant with the EU MDD or EU AIMDD with a valid declaration and CE marking can be placed on the Great Britain market up until the sooner of the expiry of the certificate or 30 June 2028;
 - in vitro diagnostic medical devices compliant with the EU IVDD can be placed on the Great Britain market up until the sooner of the expiry of the certificate or 30 June 2030, and
 - general medical devices, including custom-made devices, compliant with EU MDR and IVDs compliant with the EU IVDR can be placed on the Great Britain market up until 30 June 2030.
- In addition, MHRA announced that medical device certificates that have been extended in the EU by Amendment to EU MDR will also be recognized as valid for placing CE marked devices on the Great Britain market.



SaMD and AI (1/3)

- Software with a medical purpose must comply with EU MDR ,

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

- (1) 'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
 - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
 - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
 - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
 - providing information by means of *in vitro* examination of specimens derived from the human body, including organ, blood and tissue donations,

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

- Rule 12 Annex IX MDD: risk class I / Rule 11 Annex VIII MDR: risk class IIb

SaMD and AI (2/3)

- **Timeline:** Commission Proposal of an Artificial Intelligence Act in 2021 → Entry into force end of 2023 → Date of Application 2026

- **Legal definition of AI in the Commission AIA:**

For the purpose of this Regulation, the following definitions apply:

(1) ‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

- AI systems which are devices and governed by EU MDR are considered “high risk AI”
- Article 16 AIA “*Obligations of providers of high-risk AI Systems*”: QMS, TD; conformity assessment under AI, etc.
- The relation between MDR and AI Act can lead to overregulation which makes it much more difficult to place new products on the market:

SaMD and AI: Reimbursement of Digital Health Applications (3/3)

- **Germany**: reimbursement of digital medical devices via statutory health insurance is regulated in the DiGA directory ("DiGA Verzeichnis").
 - Digital health applications listed in this directory can be prescribed by physicians and psychotherapists to support the detection and treatment of diseases. The costs for the DiGA as well as for any medical services required in the context of their use are covered by the statutory health insurance.
 - The inclusion in the DiGA directory must be applied for by the manufacturer in a formal application procedure. The application is reviewed and evaluated by BfArM within three months.
- **France**: In October 2023 the French official journal published three orders which facilitate the prescription and the reimbursement of digital medical devices.
 - The system targets medical devices, duly CE marked, compliant with the GDPR, which are innovative (in particular in cancer).
 - Thanks to this system, they are reimbursed (e.g. EUR 50 par patients per month), for a temporary time (less than 1 year), until they are reimbursed with the usual system once their full dossier is filled and validated.



Questions?

9th November 2023

Dr Cord Willhoeft, LL.M.



Panel Discussion

Thursday, November 9th, 2023

Panel Discussion



Mark Gardner
Directing Attorney
Gardner Law



Sushana Vijayakumar
Principal Legal Counsel
Medtronic



Sara Kerrane
VP Intellectual Property,
Litigation & Regulatory
Counsel, Glaukos



Jeff Dennis
Global Privacy &
Cybersecurity Attorney;
Chief Privacy Officer,
Edwards Lifesciences