Transatlantic Legal-Regulatory Update: Live from the Heart of Silicon Valley

November 10, 2022

Mountain View, CA

12:30 – 4:30pm PT

GARDNER LAW

fieldfisher

Agenda

12:30 - 12:45 PM -	Program Introduction
12:45 - 1:15 PM -	Session one: FDA Violations and the Park Doctrine Threat, Amanda Johnston
1:15 - 1:45 PM -	Session two: EU Healthcare Compliance Update, Cord Willhöft
1:45 - 2:15 PM -	Session three: Pre-Approval Communications and Trial Recruitment Do's and Don't's, Mark Gardner
2:15 - 2:30 PM -	Break
2:30 - 3:00 PM -	Session four: International Data Transfers: How can international businesses ensure compliance?, Oliver Süme
3:00 - 3:30 PM -	Session five: Cybersecurity, Paul Rothermel
3:30 - 4:00 PM -	Session six: EU MDR update and UK/Swiss Market Entry, Cord Willhöft
4:00 - 4:30 PM -	Session seven: Panel Discussion, Amanda Johnston, Mike Pisetsky, Alaleh Nouri & Bill Revelos

GARDNER LAW

fieldfisher

Program Introduction

- Welcome to the program.
- Review of agenda.
- CLE event is being recorded and the recording will be available after the event.
- Slides are available during the presentation via the handout window on the control panel.
- Remote participants are muted and can submit questions via the question function on the control panel. Questions can be submitted throughout the program.
- 3.5 credits have been approved by the Minnesota Board of Continuing Legal Education. Information will be sent out after the CLE to self report in other states.

Session One:
FDA Violations and the Park Doctrine Threat

Speaker:

Amanda Johnston, J.D.,
R.A.C. Managing Attorney
ajohnston@gardner.law
+1 (763) 639-6951 mobile

Amanda Johnston, JD, RAC, Managing Attorney, Gardner Law, specializes in counseling medical technology and pharmaceutical companies on FDA law, regulatory submissions and strategy, healthcare compliance programs, and fraud and abuse laws. Prior to practicing at Gardner Law, she was the Compliance Officer at Coloplast Corp, in Regulatory Affairs at Medtronic (Star of Excellence Award winner), and in Compliance at UnitedHealth Group. Amanda is an Adjunct Professor of Law at Mitchell Hamline School of Law where she teaches Drug & Device Law.

GARDNER LAW

fieldfisher

Agenda

- FDA Violations & Enforcement Mechanisms
- The *Park Doctrine*
- Use of the *Park Doctrine*
- DOJ Perspective on Individual Accountability
- Predictions & Recommendations
- Questions?

Federal Food, Drug and Cosmetic Act (FDCA)

- Passed by Congress in 1938, giving authority to the U.S. Food and Drug Administration ("FDA") to oversee the safety of food, drugs, and cosmetics.
  - Regulates how drugs and devices are **manufactured and promoted**
- FDA is responsible for protecting public health

What happens if FDA regulations are not followed?

Misbranding

- **Generally, this means something is wrong with the words used to describe/promote the device**
- Promotion of unapproved devices, uses, features
- False, misleading, untruthful, not balanced with risks
- Inadequate directions for use

Adulteration

- **Generally, this means something is wrong with the way the product is made**
- Device company with no or inadequate QMS
- Manufacturing issues

Poll Question

TRUE OR FALSE:

As an executive, you can be held criminally liable for your employees' misconduct, even if you do not know about the misconduct.

The *Park Doctrine*

United States v. Dotterweich, 320 U.S. 277 (1943)

Facts

- Joseph Dotterweich (President & CEO of Buffalo Pharmacol Company)
- Company bought drugs and repackaged/shipped them under their own label, and in some cases, the labels were incorrect
- Dotterweich had no knowledge that the drugs were shipped into interstate commerce

Holding

- Supreme Court held that individuals can be held criminally liable for FDCA violation "without consciousness of some wrongdoing" if they have a "responsible relationship to, or [has] a responsible share in, violations"

Rule

- Corporate officer can be held criminally liable under the FDCA when he has "responsibility and authority either to prevent in the first instance, or promptly to correct, the violation complained of" and fails to do so

United States v. Park, 421 U.S. 658 (1975)

Facts

- Mr. Park was President and CEO of Acme Markets, Inc., a national retail food chain with 36,000 employees, 874 locations, 16 warehouses
- FDA inspectors discovered rat infestation in warehouses
- Acme failed to address the problem, Park knew of the problems
- Acme and Park were both charged for FDA violations related to holding food in rodent-infested warehouses (adulterated food)
- Acme pled guilty, but Park went to trial

Holding

- The Supreme Court held that Park was properly prosecuted and convicted under the FDCA for the introduction of adulterated articles into interstate commerce
- The FDCA imposes a duty to seek out and remedy violations and a duty to implement measures to prevent violations

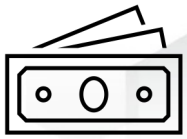
Rule

- Liability under the FDCA does not require awareness of wrongdoing or conscious fraud.
- individuals in positions of authority in businesses that affect the public health are held to a strict and rigorous standard of accountability under the FDCA.

The *Park* or Responsible Corporate Officer (RCO) Doctrine

- **Imposes strict, vicarious criminal liability upon responsible corporate officers for misdemeanor FDCA violations.**
  - No proof of knowledge, negligence, intent, or involvement needed
  - Liability based solely on RCO's duties, roles, and responsibilities

- 21 U.S.C. § 333(a)(1):
  - "Any person who violates a provision of [21 U.S.C. § 331 ("prohibited acts")] shall be imprisoned for not more than one year or fined . . .or both."
    - Prohibited acts: misbranding, adulteration, etc.
    - Misdemeanors can pile up (jail and fines)



TRUE OR FALSE:

As an executive, you can be held criminally liable for your employees' misconduct, even if you do not know about the misconduct.

Answer: TRUE.

RCOs can be held criminally liable for misdemeanor FDCA violations without proof of knowledge, negligence, intent, or involvement.

Use of the *Park Doctrine*

- ***Purdue Pharma***
  - OxyContin: misleading/false messages re: less addictive, less subject to abuse and diversion, and less likely to cause tolerance/withdrawal.
  - In 2007, executives (CEO, GC, and CMO) pled guilty to misdemeanor misbranding violation
  - No evidence that the executives were involved in or knew about misconduct; they were charged based on the fact that they were RCOs at the time of the misconduct.
- ***Synthes/Norian***
  - Bone cement product: off-label promotion, false statements
  - In 2009, three executives (President, Sr. VP, and Director of RA/CA) pled guilty to misbranding and adulteration misdemeanors as RCOs
  - Accepted pleas, but gov't presented evidence that they knew about and personally participated in misconduct

Use of the *Park Doctrine*

- ***KV Pharmaceuticals (US v. Hermelin)***
  - Manufacturing issues resulted in "super potent," oversized morphine pills
  - In 2011, CEO was convicted of misdemeanor misbranding
  - CEO did not know about the misconduct, but he had the "authority and responsibility to prevent and correct FDCA violations."
- ***Apothécure, Inc. (US v. Osborn)***
  - Osborn was the President/Director/Pharmacist of compounding pharmacy; sold high/low potency doses of pain medications resulting in 3 deaths
  - In 2012, Osborn was convicted of misdemeanor misbranding
  - He had no knowledge of the potency issues, but was responsible for procedures, equipment, and training of employees and had obligation to "prevent the misbranding."

Use of the *Park Doctrine*

- ***Jensen Farms***
  - In 2013, two principals were convicted of misdemeanor adulteration based on knowledge of conditions that resulted in contaminated cantaloupe, Listeria outbreak, and 33 deaths
  - Did not know the cantaloupe was contaminated but they knew that they had not implemented an anti-contamination procedure to prevent it
- ***Quality Egg LLC (US v. Decoster)***
  - Salmonella-contaminated eggs
  - In 2014, executives were convicted of misdemeanor adulteration
  - Did not know the eggs were contaminated, but knew of sanitation issues and did not address them
- ***Indivior PLC***
  - Suboxone Film for the treatment of opioid addiction
  - Allegations: misleading claims, encouraged prescriptions where not clinically warranted
  - In October 2020, former CEO was convicted of misdemeanor misbranding based on his role as a responsible executive who failed to prevent or correct FDCA violations
  - Strict liability FDCA misdemeanor based on position as RCO

What does *Park* mean for RCOs today?

- RCOs are in the crosshairs and could be criminally charged for misdemeanor FDCA violations, even without knowledge or intent.

- RCOs have the following duties:
  - A duty to seek out and remedy potential FDCA violations
  - A duty to implement measures that will prevent FDCA issues

- RCO liability could arise from (not exhaustive):
  - Off-label or pre-approval promotion
  - Inadequate instructions for use
  - Product defects (quality issues)
  - Manufacturing issues

The DOJ Perspective on Individual Accountability

DOJ on Individual Accountability

- September 2015 “Yates” DOJ Memo
  - Focus on individual accountability for corporate wrongdoing
  - *“One of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing.”*
- October 2021 DOJ Memo
  - Creation of “Corporate Crime Advisory Group” within DOJ
- September 2022 DOJ Memo
  - Policy revisions based on Corporate Crime Advisory Group feedback
  - Affirmed focus on individual and corporate accountability
  - *“The Department's first priority in corporate criminal matters is to hold accountable the individuals who commit and profit from corporate crime.”*

Predictions: Will we see more *Park*/RCO enforcement?

- Likely, yes, particularly in cases where:
  - Individuals/patients are harmed (e.g., defective products, patient deaths, false/misleading communications)
  - The company has QMS problems
  - The company's compliance program is insufficient
- DOJ has recently affirmed its focus on individual accountability
- A recent JAMA Editorial (September 2022) called for increased *Park* prosecutions
  - Suggests that the government is not exercising its full authority under the *Park* doctrine to sanction corporate behavior that threatens patients and public health.
  - **Concludes that enforcement under a reinvigorated *Park* doctrine could better promote the doctrine's goal of protecting patients.**

Recent Enforcement Trends: Device Quality Issues

- ***Alere***
  - July 2021, $38.75M False Claims Act settlement
  - Allegations: Alere knowingly sold defective blood coagulation monitors that produced inaccurate and unreliable results for some patients due to algorithm defect

- ***St. Jude***
  - July 2021, $27M False Claims Act settlement
  - Allegations: St. Jude knowingly sold defective heart devices; failed to disclose/fix battery issues that resulted in device failure
  - Patient brought *qui tam* case

- ***Avanos Medical***
  - In July 2021, $22M & Deferred Prosecution Agreement (DPA)
  - Criminal misbranding case
  - Allegations: Avanos falsely labeled surgical gowns, false statements to FDA

Best Practices & Recommendations

- A compliant and operational Quality Management System (QMS) is essential.
  - Invest in quality
  - Conduct internal audits, monitoring
- A robust and effective compliance program is essential.
  - Leadership training on the Park Doctrine
  - Consistent enforcement of compliance program violations
  - Instill a culture of compliance and a “speak up” culture
- Make good hiring and promotion decisions.
- Establish clear expectations related to supervisory responsibilities.
- Be proactive in identifying and addressing issues (e.g., quality, marketing).

GARDNER LAW

fieldfisher

Session Two:
EU Healthcare Compliance Update

Speaker:

Dr. Cord Willhöft, LL.M.
Partner, Life Sciences
cord.willhoeft@fieldfisher.com
+49 (0)172 881 49 96

Cord advises medical device manufacturers and pharmaceutical companies on matters of reimbursement eligibility, regulatory market access and healthcare compliance. His expertise includes the reimbursement and pricing of pharmaceuticals and medical devices in the stationary and outpatient service areas of the statutory health insurance (GKV).This includes practice assessment procedures before the Federal Joint Committee (G-BA) and negotiations with statutory health insurance companies and the GKV-Spitzenverband.

Cord's regulatory consulting practice particularly encompasses placing pharmaceuticals and medical devices on the market (conformity assessment procedures, authorisation, distribution, GDP, contracts between different parts of the supply chain), wholesale authorisations, compassionate use and individual imports, clinical trials and good manufacturing practice.

EU Healthcare Compliance Update

I. Healthcare Compliance in EU

1. Legal Regime for Healthcare Compliance in EU
2. MedTech Europe / Country Handbook
3. Product-related Advertisement (Article 7 EU MDR)

II. Update on Key Markets

1) Germany: Meal Limits, FMV, Personal Liability of General Directors
2) Italy: The Sun now also Shines in Italy
3) The Netherlands: National Solution for Direct Sponsoring
4) France: A new Charter on Medical Devices

GARDNER LAW

fieldfisher

EU Healthcare Compliance (1)

- **Legal Regime**
  - No “EU Law” for interactions with HCPs and HCOs
  - In theory: 27 Member States could mean 27 different set ups
  - Challenging situation for international operating MedTech companies

- **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)

- **However, principles for cooperation with HCPs / HCOs are the same:**
  - Principle of Transparency
  - Principle of Separation
  - Principe of Equivalence
  - Principle of Documentation
- **Useful reference / source for US legal departments:**
  - MedTech Europe Code of Ethical Business Practice (updated 28 March 2022), and
  - MedTech Europe Compliance Handbook (October 2021).

MedTech Europe
from diagnosis to cure

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

GARDNER LAW

fieldfisher

EU Healthcare Compliance (3)

New since 26th 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.

GARDNER LAW

fieldfisher

EU Healthcare Compliance (4)

"… 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;
→ **prohibition of misleading advertisement**

(b) creating a false impression regarding treatment or diagnosis, functions or properties which the device does not have;
→ **prohibition of misleading advertisement**

(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;
→ **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.
→ **prohibition of off-label advertisement**

Country Updates: Germany (1)

- **Still no German Sunshine Act**
  - No legal transparency regime in Germany, not even in the legislative pipeline
  - BVMed refers to Medtech Europe requirements (disclosure of educational grants), no further self-regulatory disclosure rules for transfer of value

- **Principle of Equivalence / Compensation and FMV**
  - HCP Compensation shall reflect FMV for the service provided, taking into consideration HCP´s qualification, expertise and experience.
  - Hourly rate of EUR 150-200 / hour for KOLs common practice
  - We now see acceptance of EUR 250 / hour by medical institutions for university professors (KOLs) for qualified medical services

Country Updates: Germany (2)

- **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
  - Currently in discussion and strongly discussed: Upgrade to EUR 75, self-BVMed guideline expected for Q1/2023

- **Personal liability of Managing Directors (GmbH)**
  - Higher Regional Court Nuremberg (30th March 2022. 12 U 1520/19): Managing directors may be personally liable if he/she fails to set up a compliance management system and this lack facilitated misconduct
  - Infringement of Section 43 (1) GmbHG / Managing Directors are committed to the well-being of the company and has to ensure the company´s long-term profitability

Country Updates: Italy & Sunshine

- **Italian Sunshine Act (Law No. 62 of 31 May 2022) entered into force on 26th June 2022**
  - The Italian MedTech Industry Association *Confindustria Dispositivi Medici* required member companies to disclose ToV to HCPs and HCOs since 2021 (reporting data from 2020)
  - Now it is mandatory to disclose ToV to HCPs and HCOs

- **Mandatory to disclose ToV if:**
  - individual transfer to HCP exceeds EUR 100
  - annual overall amount to HCP exceeds EUR 1,000
  - individual transfer to HCO exceeds EUR 1000
  - annual overall amount to HCO exceeds EUR 2,500

- **However:** Reporting obligations apply 6 months after Italian Transparent Healthcare Register has been established, i.e. approx. Q3/Q4 2023

Country Updates: The Netherlands (1)

Joint Statement on Phase-Out of Direct Sponsorships

The Global MedTech Industry Moving Together to Enhance Compliance Practices Across Europe, China, Middle East, North Africa & Asia-Pacific

January 3, 2018

- **Educational grants to HCO**
- **Educational Grant Agreement (cf. MedTech Europe Template)**
- **HCO is solely responsible to select the benefiting HCP**

GARDNER LAW

fieldfisher

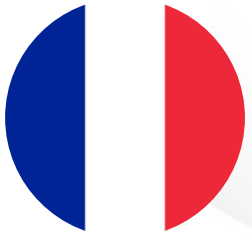
Country Updates: The Netherlands (2)

- **MedTech Europe "prohibits" direct sponsoring**
- **"Soft" transition into national industry code,** e.g. Germany "*although legally not prohibited, it is not recommended to direct sponsor…*" (BVMed Code of Conduct)
- **The Netherlands:** It is reasonable to reimburse expenses related to third-party organized educational events if
  - company contributes not more than EUR 500 per event per HCP and to a maximum of EUR 1,500 per year to that HCP, or
  - The HCP pays at least 50% of the related costs personally

GARDNER LAW

fieldfisher

Country Updates: France



- **French Charter for Presentation of Educational Information / Promotion of Medical Devices for Individual Use** (8 March 2022; Charter"):
  - Applies to all manufactures and distributors of medical devices that are reimbursed under the French national health insurance system
  - Companies must implement QMS for their presentational, informational and promotional activity (i.e. covering almost any correspondence), transitional period until March 2023

- **Restriction on company-initiated HCP visits:**
  - all visits must documented and disclosed annually on an online platform
  - disclosure of nature of visit, name of HCO/HCP, provision of samples, date of visit, etc.
  - Limit of four visits per year (!)
  - no visits during a period of public tenders

GARDNER LAW

fieldfisher

Session Three:
Pre-Approval Communications & Trial Recruitment Do's and Don't's

Speaker:

Mark Gardner, JD, MBA
Directing Attorney
mgardner@gardner.law
612-382-7584 mobile

Mark Gardner, MBA, JD, Directing Attorney, Gardner Law, has worked in FDA-regulated industry since 1999. He advises companies on a wide variety of topics including health care compliance, advertising and promotion review, FDA -regulatory, -quality, and -clinical matters, privacy, transparency reporting, and enforcement. He has worked in house with manufacturers such as Bayer Healthcare and Johnson & Johnson. Previously he worked in commercial roles, including product management, at ev3 (Medtronic), Celleration, and MedTox Laboratories (Labcorp). Mark is an Adjunct Professor of Law at Mitchell Hamline School of Law where he teaches Drug & Device Law, sits on the Health Law Institute Advisory Board, and serves as a judge and coach for student competitions.

GARDNER LAW

fieldfisher

Poll question—Pre-Approval Communications

Does your company have a product pending FDA approval?

Yes or No?

GARDNER LAW

fieldfisher

Statutory Framework for Unapproved Products

- Failure to gain approval causes products that are promoted or commercialized and introduced into interstate commerce to be misbranded and/or adulterated under the U.S. Federal Food, Drug, and Cosmetic (FD&C) Act (*See* 21 U.S.C. § 301 et seq.)
- **Drug**
  - Under the law, "No person shall introduce or deliver for introduction into interstate commerce any new drug, unless an approval of an application…is effective with respect to such drug" (*See* 21 U.S.C. § 355(a))
- **Device**
  - In order to market a Class I, II, or III medical device intended for human use, for which a Premarket Approval application (PMA) is not required, a 510(k) must be submitted to FDA unless the device is exempt from 510(k) requirements of the FD&C Act
  - Pre-market approval of certain medical devices, e.g., high-risk devices, is required (*See* 21 U.S.C. § 360e(a))

Investigational Products are Not Approved, Why Can They Be Introduced Into Interstate Commerce?

Exceptions exist for shipping into interstate commerce investigational drugs and medical devices that have not yet gained FDA approval

A drug can be shipped under an FDA-approved investigational new drug (IND) application (*See* 21 U.S.C. § 355(i); 21 C.F.R. 312)

The same is true for an investigational device under an FDA-approved investigational device exemption (IDE) (*See* 21 U.S.C. § 360j(g); 21 C.F.R. 812)

Despite being able to ship such investigational products into interstate commerce, sponsors (and investigators) researching such products are **strictly barred by regulation** from **promoting** investigational products as safe or effective, or **commercializing** such investigational products

Other Labeling Considerations

The FD&C Act prohibits statements about drugs and medical devices that are "false or misleading in any particular" (*See* 21 U.S.C. § 352(a))

- FDA may conclude that statements that **pre-promote** a product are false and/or misleading

A drug or device is also misbranded under the FD&C Act if unaccompanied by labeling containing adequate directions for respective intended use(s) (*See* 21 U.S.C. § 352(f)(1), 331(a))

What is the Difference Between: Pre-Approval ***Communication*** & Pre-Approval ***Promotion***

Pre-Approval *Communication*

- Discussing a product in a non-promotional/non-commercial fashion before it is FDA-approved, or during the pendency of FDA review

Pre-Approval *Promotion*

- Promoting and/or commercializing* a product, e.g., claiming it is safe, effective, economical, superior, etc., before or without FDA-approval of such claims

* For purposes of this presentation, promotion and commercialization are collectively "promotion"

What are Some Forms Pre-Approval Promotion Can Take?

Sell sheets	Product videos	Patient testimonials	Convention booths
Websites	Product brochures	Search engine promotions	Emails
Product mailings	TV and print advertisements	Training materials	Taking orders for unapproved products

GARDNER LAW

fieldfisher

Issues with Promoting Prior to FDA Approval

Regulator perspective

- Can put American public at risk
- People may develop misconceptions or unsubstantiated beliefs about the safety or effectiveness of a product

Business perspective

- Some view promoting a product that lacks FDA-approval as a fool's errand
- Selling something that's not available

What can happen to someone if they promote a product before approval?

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE | Thursday, April 14, 2011

Former InterMune Ceo Sentenced for False & Misleading Statements Related to Pulmonary Fibrosis Drug's Clinical Tests

SAN FRANCISCO – W. Scott Harkonen, M.D., the former chief executive office (CEO) of InterMune Inc., was sentenced Wednesday before U.S. District Court Judge Marilyn Hall Patel for wire fraud relating to the dissemination of false and misleading statements about the results of a clinical trial of InterMune's drug Actimmune. Judge Patel sentenced Harkonen to three years' probation, with six months of home confinement. He was ordered to pay a $20,000 fine and to perform 200 hours of community service. In September 2009, after a seven-week trial, a jury convicted Harkonen of wire fraud for the creation and dissemination of false and misleading information about the efficacy of Actimmune (Interferon gamma-1b) as a treatment for idiopathic pulmonary fibrosis (IPF).

Continued from the DOJ press release…

Evidence at trial further showed that Harkonen caused InterMune to issue a false and misleading press release publicly announcing the results of a clinical trial of Actimmune for the treatment of IPF on Aug. 28, 2002. Although the clinical trial had failed, InterMune's press release falsely stated that the results of the clinical trial established that Actimmune helped IPF patients live longer. The headline of the press release read, "InterMune Announces Phase III Data Demonstrating Survival Benefit of Actimmune in IPF," with the subheading "Reduces Mortality by 70% in Patients With Mild to Moderate Disease."

PHARMACEUTICALS

‘Fast Money’ faux pas: Firm draws FDA warning, DOJ subpoena

PUBLISHED MON, JAN 13 2014•4:25 PM EST | UPDATED MON, JAN 13 2014•4:40 PM EST

Dan Mangan
@_DANMANGAN

Screen shot of Marc Beer on CNBC
Source: CNBC

Hot biotech company Aegerion Pharmaceuticals found out the hard way that enthusiastic comments by its CEO about its breakthrough cholesterol drug Juxtapid could lead to unwanted attention from federal drug regulators.

The Food and Drug Administration accused CEO Marc Beer of "misbranding" Juxtapid by claiming it "is intended for new uses, for which it lacks approval and for which its labeling does not provide adequate directions for use," according to an FDA warning letter sent to the Cambridge, Mass.-based company.

The FDA claimed Aegerion made "serious" violations after Beer went too far in his comments in two separate appearances on CNBC's "Fast Money" and left the impression that Juxtapid could be used alone as a treatment for a rare genetic disease and that it could tackle heart conditions, and also that he failed to disclose the potentially serious side effects from the drug.

The company disclosed last Thursday that it had received a Justice Department subpoena for documents relating to Juxtapid's sale and marketing, a revelation that sent the company's stock dropping sharply. It is not clear if that subpoena was spurred by the FDA warning over Beer's "Fast Money" remarks, or not—but the company suggested it was not.

FDA spokeswoman Tara Goodin told CNBC.com in a prepared statement on Monday: "Regardless of the media or venue used to disseminate promotional messages about prescription drugs, pharmaceutical companies undermine the drug approval process and may put the public at risk when they promote drugs for uses that have not been proven safe and effective."

Communications Generally Allowed by FDA Prior to Approval

- Truthful and non-misleading product communications that *do not* cross the line into "promotion" or "commercialization" about an un-approved product are generally tolerated by the government
- Some rules and considerations:
  - No branded promotion
  - Be mindful of colors, fonts, and design elements used—cannot match branded product
  - Medical Affairs staff should participate in scientific exchange, not commercial staff
  - Consider disclaimers (disclose investigational status), maintain balance, disclose limitations in data and risks
    - "CAUTION – Investigational device. Limited by Federal (or United States) law to investigational use." 21 C.F.R. 812.5.
  - Audience, communication channel, content, and timing are important factors to consider

Non-Promotional Communications Examples

- Press releases (e.g., regarding first-in-human implants)
- Investor communications (no promotion)
- Market research (subject to blinding among other requirements)
- Corporate communications (not an end-around on prohibitions)

GARDNER LAW

fieldfisher

General Rules To Follow

Do:

- Script and have communications reviewed by qualified medical, legal, and regulatory professionals before sharing
- If sharing data, let it speak for itself
- Communicators should disclose relationship to company

Avoid:

- Hyperbole or unsubstantiated claims
- Colorful adjectives
- Promotional brand names/branding
- Comparisons with competitive products/treatments

Scientific Exchange

FDA does not prohibit scientific exchange communications between medical professionals so long as the communication is:

Not promotional	Not false or misleading	Balanced and complete (i.e., discloses material facts/data)	Accompanied by appropriate disclosure

FDA will look at facts/circumstances, including frequency, context, audience, method (proactive or reactive) of communications

Examples

Investigator presentations (e.g., phase 3 data presented at a medical conference)	Medical Affairs function issuing responses to unsolicited requests and disseminating publications	Medical Affairs section of exhibit booth	Scientific advisory boards (e.g., discussions about clinical trial strategy)

GARDNER LAW

fieldfisher

Aspects of Clinical Data can be Discussed Via Scientific Exchange

Acceptable topics:

- condition under study and/or intent of the research
- study design
- primary and secondary endpoints
- factual data on safety and effectiveness
- mechanism(s) of action
- product design
- constituents
- patient inclusion/exclusion criteria

When disclosing data include the "n", p-values, and confidence intervals

Share the good, bad, and ugly—do not hide the ball when it comes to unflattering data

Where appropriate, balance data with safety information

Avoid comparisons—unless an investigation relates to a head-to-head trial

Disease Awareness Examples

Disease awareness communications to patients or providers

- Not an opportunity to disparage competing therapies
- Not an opportunity to make unbalanced comparisons to competing therapies

Do not include:

- Product discussion
- Any branding in any way, shape, or form
- Any implied promotional claims

Pre-approval Communications with Payors

Provision of certain types of information to payors, value analysis committees, formulary committees, pharmacy and therapeutic committees, and similar entities

- Examples: product information, indication sought (trial protocol, patient population, endpoints), anticipated timeline for approval, product pricing, related programs and services, factual data from studies

Must follow parameters outlined in FDA guidance; For example, include:

- What product is NOT approved for
- What product is approved for (if applicable)
- Product development stage
- Disclose limitations in data

Displaying Devices Before Approval

FDA Guidance

Note: this guidance does not reference PMA devices

"A firm may advertise or display a device that is the subject of a pending 510(k) -- in the hope that FDA will conclude that the device is substantially equivalent to a pre-amendments device"

"a firm may not take orders, or be prepared to take orders, that might result in contracts of sale for the device unless limited to research or investigational use."

FDA Notice of Availability Guidance

Prepare a “notice of availability” for a medical device

For obtaining clinical investigators to further scientific research

No claims that device is safe or effective

Sponsors and investigators can use a notice of availability to “make known through a notice, publication, display, mailing, exhibit, announcement, or oral presentation the availability of an investigational device for the purpose of obtaining clinical investigators to participate in a clinical study”

Must follow parameters outlined in FDA guidance

Hypothetical: Tradeshow

- Your Chief Commercial Officer wants to display a medical device at the company booth at an upcoming tradeshow. The booth captain, a product manager, plans to put a sticker on the device disclosing that it is pending FDA 510(k) clearance and is not approved. If anyone asks about it, an engineer will be on hand to explain how the device functions. No promotion will take place. Only factual information will be conveyed. Orders will be taken for the new product so that it can be shipped once it is cleared. The company needs to hit its quarterly goals so getting this early jump is going to help the bottom line a lot.
- Is this okay?

Hypothetical: Press Release

- Your CEO is raising money. She wants to make sure current and prospective investors know how great things are going at the company. She wants to issue a press release right away recently published clinical research for an investigational drug that is currently under FDA review. She includes quotes from physician investigators that contain the words “game-changer”, “safe”, “effective”, “ground-breaking”, “remarkable results”, in the draft press release.
- Is this okay?

Poll question—Trial Recruitment

Is your company currently recruiting patients for a clinical trial?

Yes or No?

Trial Recruitment Do's and Don'ts

- Communications with prospective patients about the study device or drug may trigger the informed consent process
  - Consider what is being shared
  - Basic information may not trigger the informed consent process
- Institutional review board (IRB) review of recruitment materials is required
  - Consider here again what is being shared and sponsor obligations
- Decide what will be covered from a financial perspective
  - OIG Advisory Opinion (22-05) may present opportunities for cost-sharing, depending on the facts
- Make sure your clinical trial agreement (CTA) subject injury provisions line up with the informed consent form (ICF) and Medicare rules

Rules for research payments

FMV (fair market value) assessment

- Personal Services and Management Contracts Safe Harbor
- Research payments must be paid at FMV and cannot be a reward for purchases or referrals
- Review all:
  - Payments in budget to make sure they are legitimate
  - Request for payments
- Consider what the basis is to set payments? (e.g., Medicare rates, purchased data)
- What about "overhead" payments? How much is too much?

Carefully draft your CTA and budget

- Payments should be itemized
- Make payments to the institution and not the HCP
- Consider triggers for payment—if milestones are used then make sure they are achieved before paying a tranche
- *See* our website for a recent presentation about negotiating CTAs

Recruitment Bonuses

- It is okay to pay for legitimate recruitment efforts
  - Pay fair market hourly rates negotiated at arm's-length
- Is it okay to pay customer clinical trial staff a cash or in-kind bonuses (a.k.a., a bounty) in exchange for enrolling patients into a clinical trial?
  - No. Do not pay bonuses, bounties, spiffs, etc., for recruiting
- Consider:
  - "The American Medical Association asserts that "*offering or accepting payment for referring patients to research studies (finder's fees) is unethical*."
  - The AMA's prohibition of finder's fees in clinical research extends beyond its own membership, as many other entities require physicians to follow AMA's code of ethics in its entirety
  - State laws also (e.g., OH)
  - IRB rules
  - Offering Incentives, OEI-01-97-00195: Recruiting Human Subjects: Pressures in Industry-Sponsored Clinical Research
  - Recruitment Incentives, OEI-01-97-00196: Recruiting Human Subjects: Sample Guidelines for Practice
  - HHS Guidance: Financial Conflict of Interest

GARDNER LAW

fieldfisher

Session Four:
International Data Transfers: How can international businesses ensure compliance

Speaker:

Oliver Süme
Partner, Technology & Data
oliver.sueme@fieldfisher.com
+49 (0)40 878 869 82 17

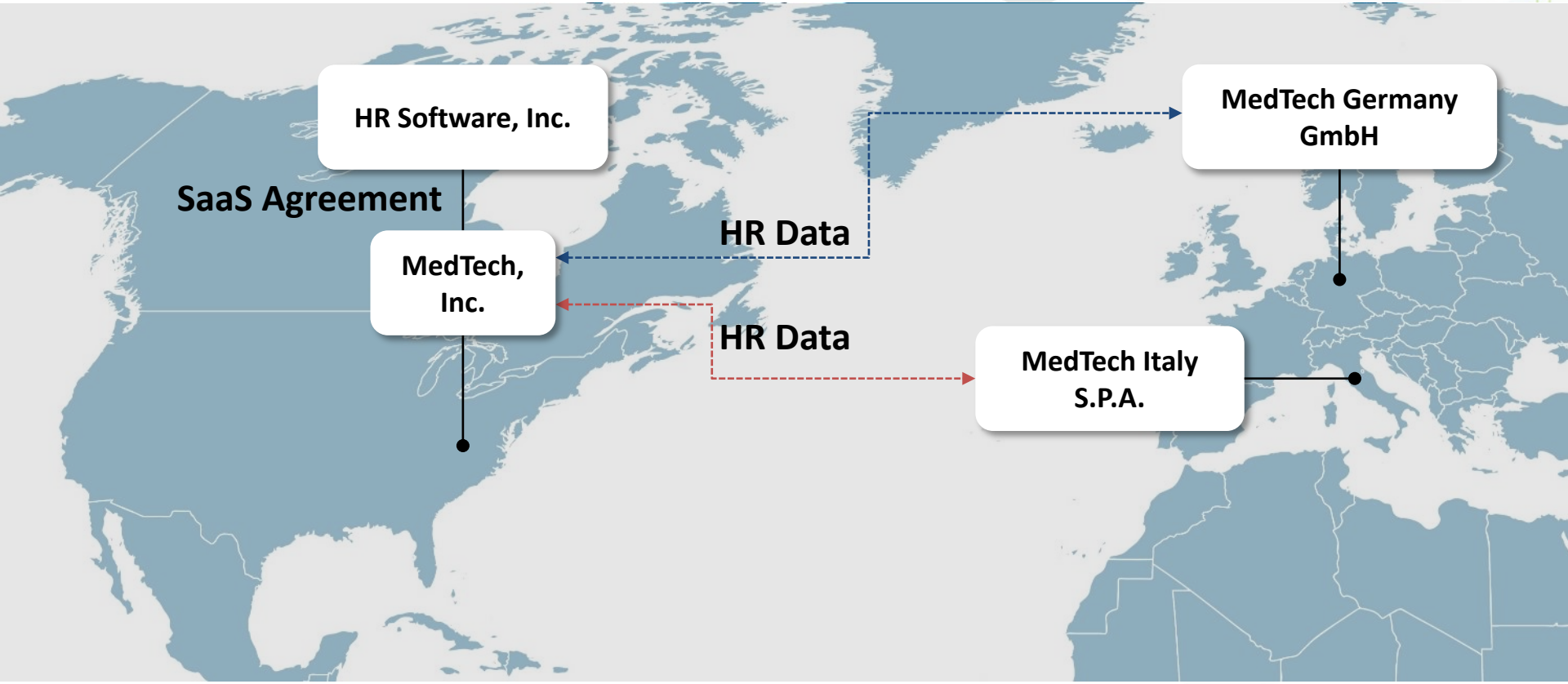
Oliver advises clients on all areas of law affecting information technology and digitalisation, with a focus on IT contracts, data protection, IT security and e-commerce.

Oliver has a particular focus on advising international life science companies on data protection and GDPR compliance. He also helps businesses and associations involved in legal and political decision-making on digitalisation at national and European levels. He is familiar with the legislative processes for national and EU levels.

GARDNER LAW

fieldfisher

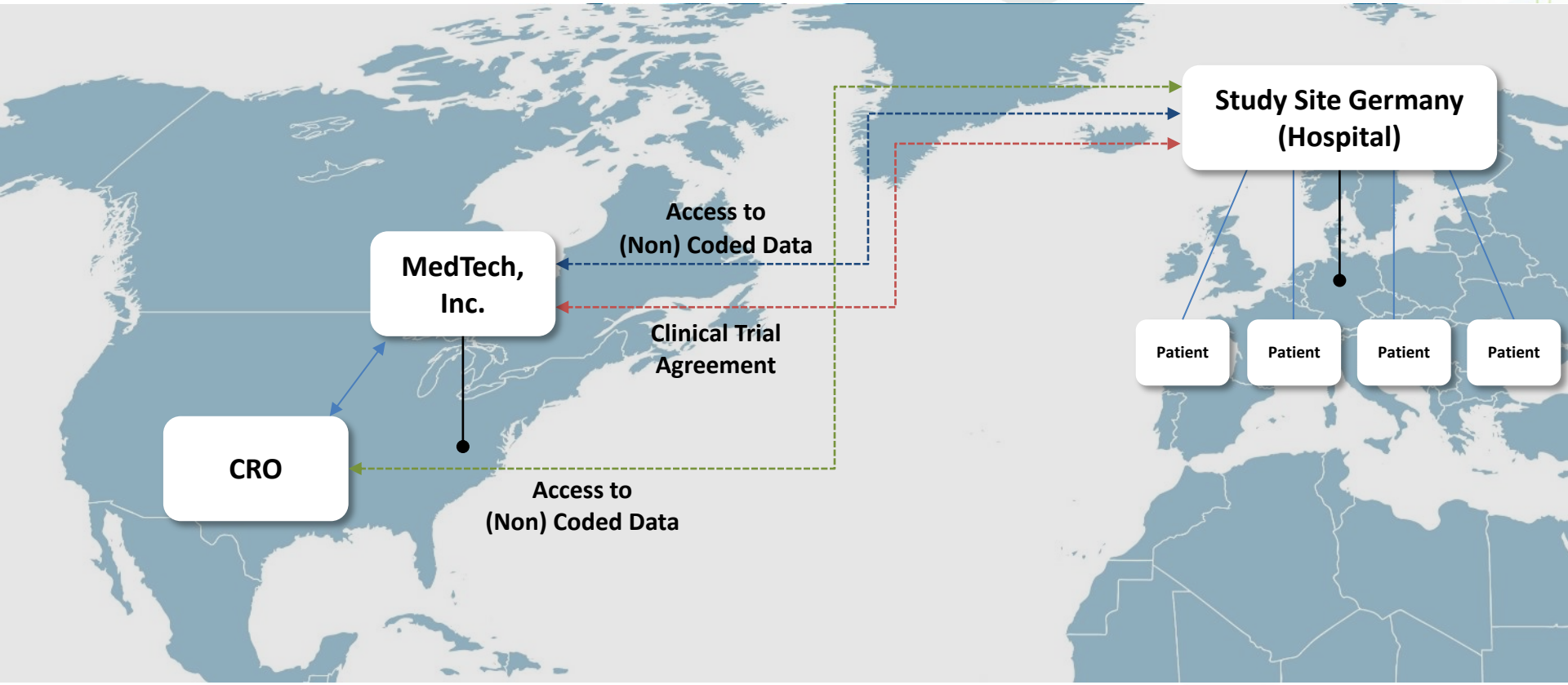
International Data Transfer – HR Data



GARDNER LAW

fieldfisher

International Data Transfer – Clinical Trial Data



GARDNER LAW

fieldfisher

Legal grounds for international data transfer under GDPR

Adequancy Decision

All EEA Countries

Approved countries (e.g. Argentina, Canada, Japan, Republic of Korea,Switzerland)

Appropriate Safeguards

Standard Contract Clauses (SCC)

Approved code of conduct

Binding Corporate Rules

- **Intra group** transfers only
- Approval by competent **DPA** required

Derogations

- **Consent** of individual
- **Contractual obligation** for individual
- **Vital interests** of individual

GARDNER LAW

fieldfisher

“Schrems 2” decision of the European Court of Justice

- **July 2020:** Judgment of the EU's highest court about the requirements for international data transfers, particularly to the US.
- The **EU-US Privacy Shield** was invalidated but **Standard Contractual Clauses** (**"SCCs"**) can still be used!
- However, it must also be checked that importing countries provide “essentially equivalent” protection, particularly regarding government surveillance. This requires to carry out a “**Transfer Impact Assessment**”.
- If no essential equivalence, then “supplementary measures” must be implemented so that essential equivalence is reached.

What was the regulatory response to “Schrems 2”?

- “The **European Data Protection Board** (“EDPB”) provided **recommendations**, including how to produce transfer impact assessments (“TIAs”) and what supplementary measures might be sufficient.
- At nearly the same time, the European Commission released **new SSCs**. These codified the need for a TIA.
- Until recently there has been only **limited enforcement action** by regulators with regard to international data transfers.

GARDNER LAW

fieldfisher

The old SCCs versus the new SCCs

Old SCCs

3 sets

- Controller to Controller (x2)
- Controller to Processor

Bipartite agreements, capturing only relationship between two parties

New SCCs

1 set

- **Mod 1:** Controller to Controller
- **Mod 2:** Controller to Processor
- **Mod 3:** Processor to Subprocessor
- **Mod 4:** Processor to Controller

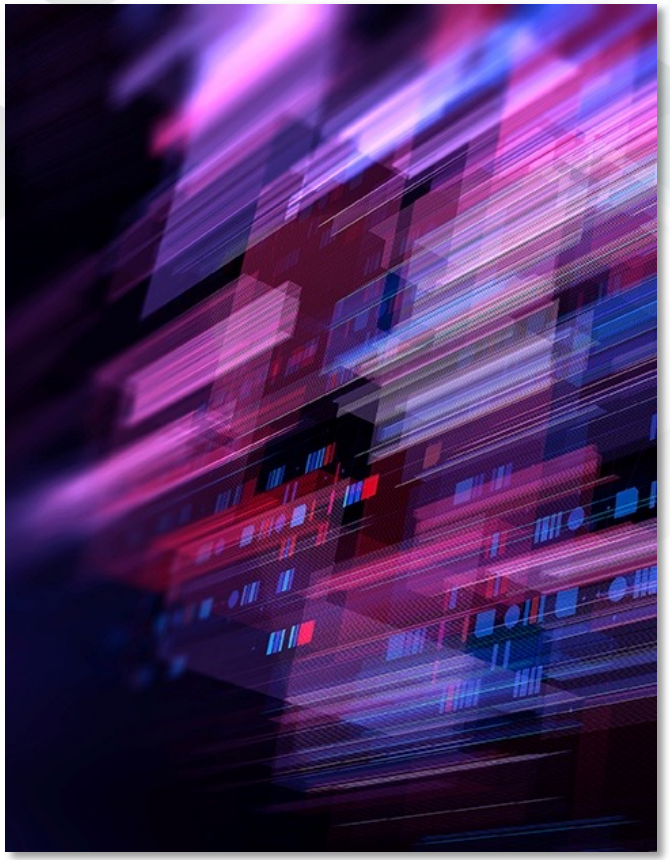
"Docking Clause":
Multiple data exporting parties can contract and new parties can be added

GARDNER LAW

fieldfisher

Supervisory authority views on use of the SCCs

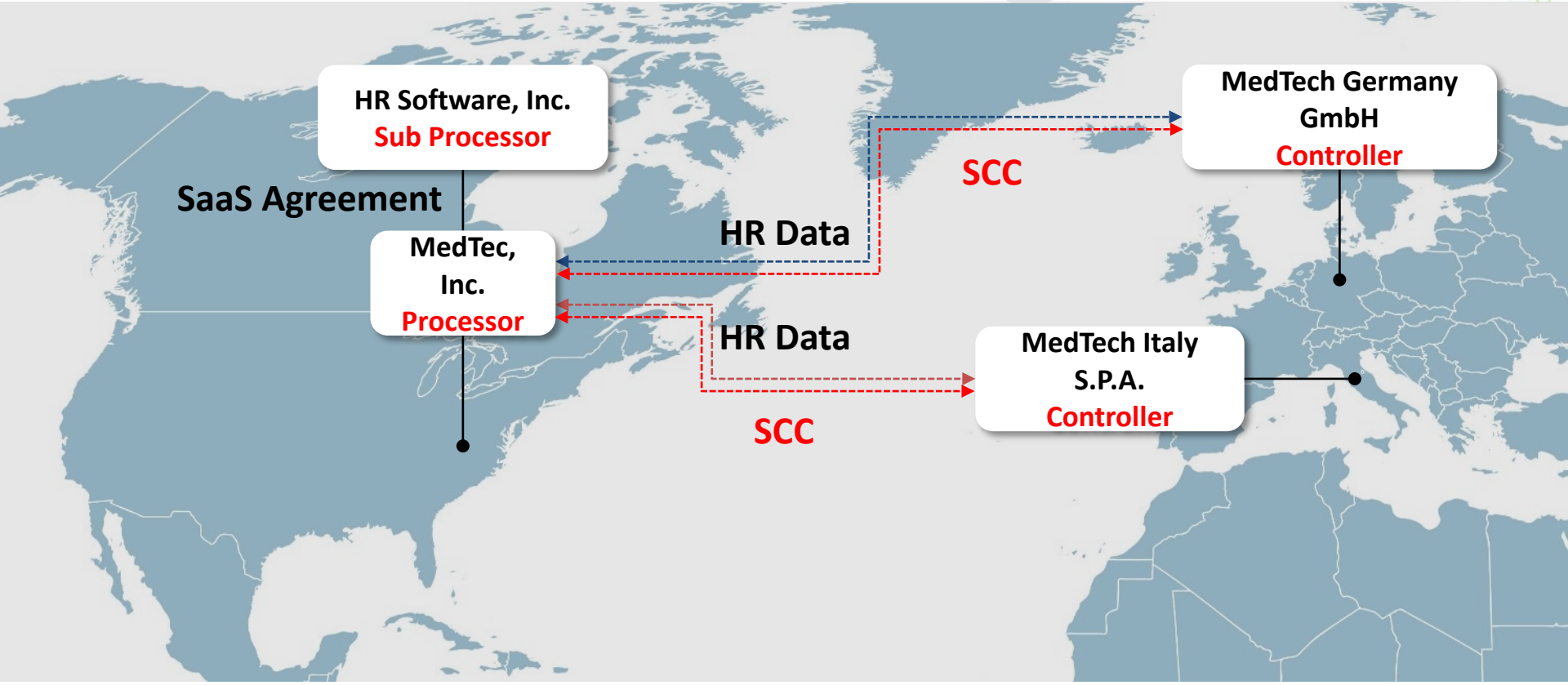
- Supervisory authorities will expect that the **new SCCs are already being used** for all new data processing agreements since September 2021.
- Supervisory authorities also expect that companies have entered into the new SCCs for existing DPAs **before the 27 December 2022 deadline**.
- The new SCCs come with the **additional obligation to create a Transfer Impact Assessment (TIA).**



GARDNER LAW

fieldfisher

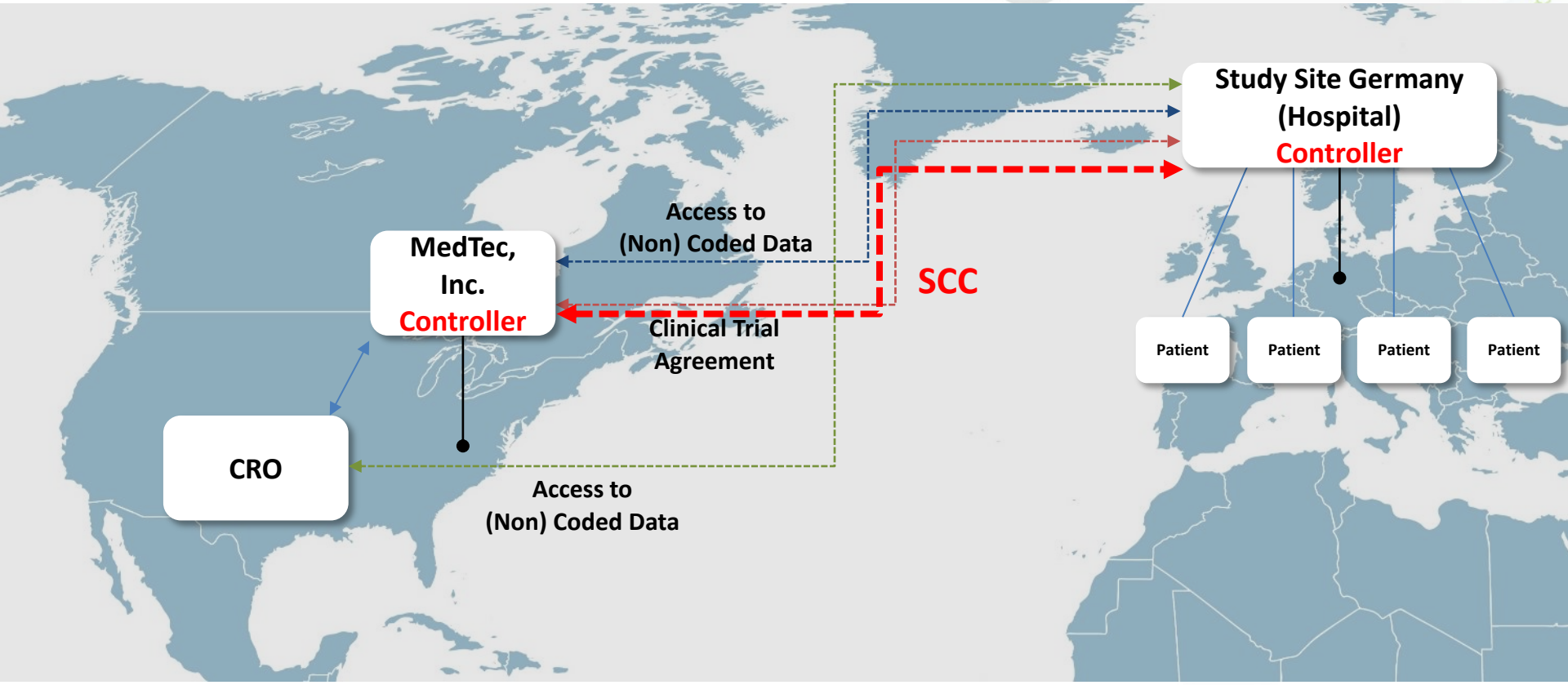
Standard Contractual Clauses secure Data Transfer



GARDNER LAW

fieldfisher

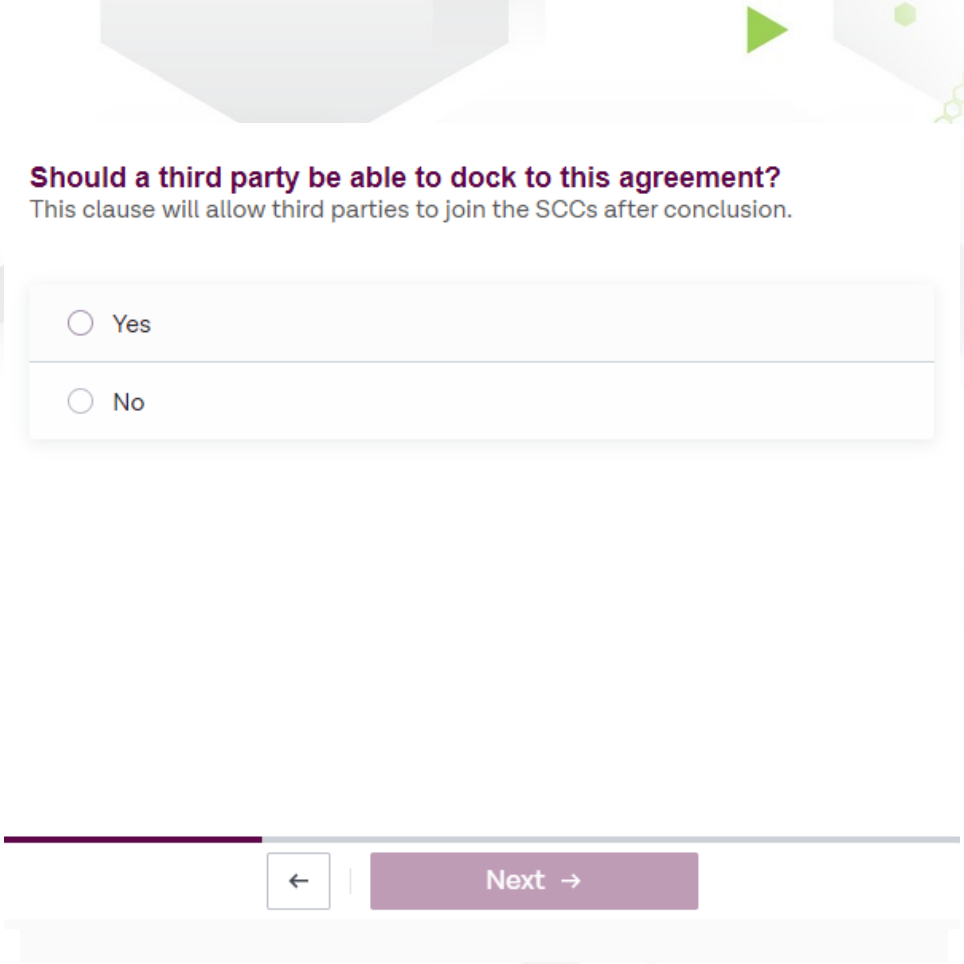
International Data Transfer – Clinical Trials



GARDNER LAW

fieldfisher

Legal Tech can help: MySCCCreator



GARDNER LAW

fieldfisher

Are the SCC's all about "Standards"? No!

- **Data flows and role of parties as controller or processor** have to be considered before putting together the adequate SCC modules
- **Legal Tech tools** like *MySCCcreator* can help to do so
- However, information about data categories, purpose of data transfers, retention periods and description of the technical and organisational measures implemented by the data importer need to be **filled out individually**!
- Clause 14 requires a **Data Transfer Impact Assessment (TIA)** and documentation of **Supplementary Safeguards**

GARDNER LAW

fieldfisher

Schrems 2: Recommendations from European Data Protection Board (EDBP) on Transfer Impact Assessments

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Version 2.0

Adopted on 18 June 2021

Recommendations published in June 2021 provide exporters with a series of **steps to follow**, potential sources of information, and some examples of supplementary measures that could be put in place.

EDPB provides a roadmap of the steps to take in order to find out if a company as a data exporter needs to put in place supplementary measures to be able to legally transfer data outside the EEA.

GARDNER LAW

fieldfisher

Transfer Impact Assessment (TIA) according to EDPB recommendations:

Step 1: Know your transfers.

Step 2: Identify the transfer tools you are relying on.

Step 3: Assess whether the **Article 46 GDPR transfer tool** you are relying on is effective in light of all circumstances of the transfer.

Step 4: Adopt **supplementary measures**.

Step 5: Procedural steps if you have identified **effective supplementary measures**

Step 6: Re-evaluate at appropriate intervals 

GARDNER LAW

fieldfisher

Supplementary Measures according to EDPB recommendations

- **Supplementary Measures** may have a contractual, technical or organizational nature;
- **Contractual and organizational measures** alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices;
- **Use strong encryption** before transmission;
- **Encryption algorithm and its parameterization** (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities;
- **Keys are reliably managed** (generated, administered, stored);
- **Keys are retained solely under the control of the data exporter**.

The new EU-U.S. Data Privacy Framework

- On Oct. 7, President Biden signed an Executive Order, implementing the successor agreement of the former Privacy Shield ("*EU-U.S. Data Privacy Framework*")

- **Three key components:**
  - (1) commercial data protection principles to which U.S. organizations may self-certify
  - (2) Presidential Executive Order
  - (3) DOJ regulations

THE NATIONAL LAW REVIEW

President Biden Issues Executive Order Providing for New EU-U.S. Data Privacy Framework

Wednesday, October 26, 2022

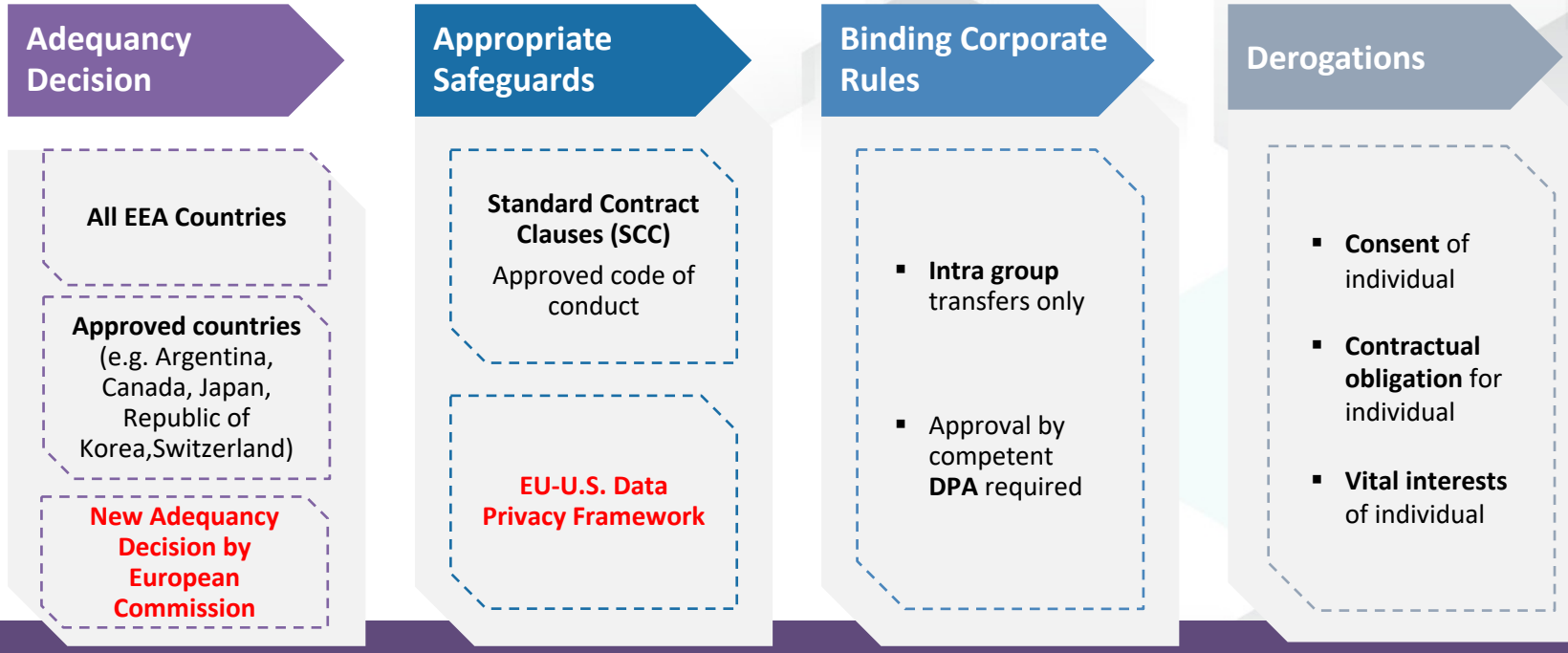
On October 7, 2022, President Biden signed Executive Order (EO) 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," which provides a new framework for legal data transfers between the European Union (EU) and the United States. The legal basis for transatlantic data transfers has been uncertain since 2020 when the European Court of Justice (ECJ) in *Schrems II* invalidated the EU-U.S. Privacy Shield Framework to transfer data from the EU and other European Economic Area (EEA) countries to the United States.

This follows the European Commission's and the United States' announcement in March 2022 that they had reached an agreement in principle on the new EU-U.S. Data Privacy Framework to facilitate transatlantic data flows.

GARDNER LAW

fieldfisher

How does the new DPF fit into the GDPR system for inmternational data transfer?



GARDNER LAW

fieldfisher

What will the DPF ensure?

- **Signals intelligence collection may be undertaken only where necessary** to advance legitimate US national security objectives. Must not disproportionately impact the protection of individual privacy and civil liberties
- **EU individuals may seek redress** from a new multi-layer redress mechanism that includes an independent Data Protection Review Court .
- **U.S. intelligence agencies will adopt procedures** to ensure effective oversight of new privacy and civil liberties standards.
- **Participating companies that take advantage of the DPF** will continue to be required to adhere to the Privacy Shield Principles, including the requirement to self-certify their adherence to the Principles through the U.S. DoC.

Next Steps and timeline

- **European Commission** will have to initiate an Adequacy Decision according to Art. 45 sec. 3 GDPR.
- **European Data Protection Board (EDPB)** will have to submit its opinion.
- **European Member States** will also have to submit their position.
- **EU-U.S. Data Privacy Framework** will not enter into force before Summer 2023.

GARDNER LAW

fieldfisher

Will the new DPF be challenged again in front of the ECJ?

noyb

News Projekte Ressourcen Jetzt Unters

HOME > NEWS > NEW US EXECUTIVE ORDER UNLIKELY TO SATISFY EU LAW

New US Executive Order unlikely to satisfy EU law

Oct 07, 2022

We are now working on an in-depth analysis, which will be published on noyb.eu in the next days.

First reaction: Executive Order on US Surveillance unlikely to satisfy EU law

More than six months after an "agreement in principle" between the EU and the US, US President Joe Biden has signed the long-awaited Executive Order that is meant to respect the European Court of Justice's (CJEU) past judgments. This is meant to overcome limitations in EU-US data transfers. The CJEU required (1) that US surveillance is *proportionate* within the meaning of Article 52 of the Charter of Fundamental Rights (CFR) and (2) that there is access to *judicial redress*, as required under Article 47 CFR. Biden's new Executive Order seems to fail on both requirements. There is continuous "bulk surveillance" and a "court" that is not an actual court.

GARDNER LAW

fieldfisher

GARDNER LAW

fieldfisher

Session Five: Device Cybersecurity and State Privacy Notes

Speaker:

Paul Rothermel, **JD, CIPM**
Associate Attorney
prrothermel@gardner.law
651.364.7514 mobile

Paul Rothermel specializes in privacy and cybersecurity, including HIPAA, 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 issues related to privacy program implementation, clinical research, innovative health care technologies, and vendor management. Before that, Paul was an Associate General Counsel for the State of Minnesota, where he counseled on state and federal privacy laws, including HIPAA implementation. Paul earned his J.D. from William Mitchell College of Law and his B.A. in History at the University of Northwestern-St. Paul. Paul is also a Certified Information Privacy Manager (CIPM) through the International Association of Privacy Professionals.

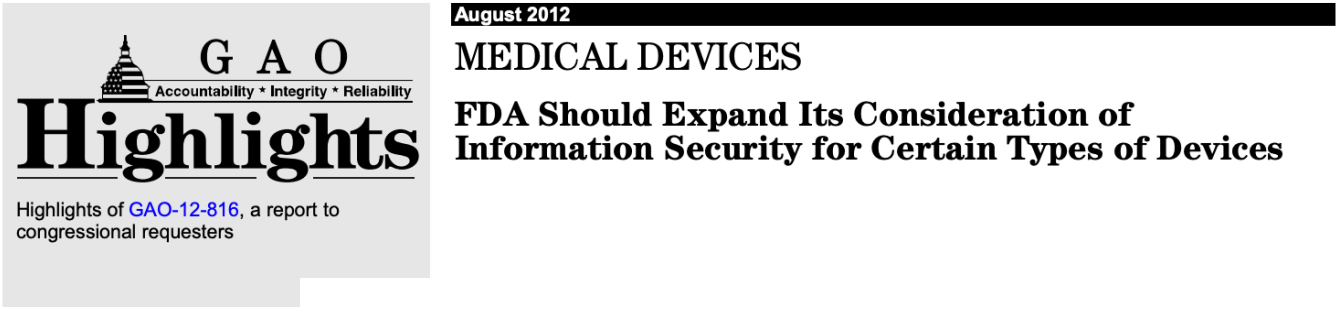
Overview

- Medical device cybersecurity trends
- FDA draft guidance
- Reporting requirements
- Other cybersecurity considerations and takeaways
- State privacy notes

Poll Question

Does your company have a device with cybersecurity risks?

In the news...



GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-816, a report to congressional requesters

August 2012

MEDICAL DEVICES

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

Cheney's defibrillator was modified to prevent hacking

Dana Ford, CNN

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

SHARE | TWEET | LINKEDIN | PIN IT | EMAIL | PRINT

Date Issued:

January 9, 2017

GARDNER LAW

fieldfisher

Device cybersecurity... And the FBI?

Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities

Summary

The FBI has identified an increasing number of vulnerabilities posed by unpatched medical devices that run on outdated software and devices that lack adequate security features. Cyber threat actors exploiting medical device vulnerabilities adversely impact healthcare facilities' operational functions, patient safety, data confidentiality, and data integrity. Medical device vulnerabilities predominantly stem from device hardware design and device software management. Routine challenges include the use of standardized configurations, specialized configurations, including a substantial number of managed devices on the network, lack of device embedded security features, and the inability to upgrade those features.

FDA on medical device cybersecurity

Focuses on impact to safety and effectiveness of medical devices:

"With the increasing integration of wireless, Internet- and network- connected capabilities, portable media (e.g., USB or CD), and the frequent electronic exchange of medical device related health information, the need for robust cybersecurity controls to ensure medical device safety and effectiveness has become more important."

Addresses confidentiality of device data, but with focus on patient safety:

"Manufacturers should ensure support for the confidentiality of any/all data whose disclosure could lead to patient harm (e.g., through the unauthorized use of otherwise valid credentials, lack of encryption)."

GARDNER LAW

fieldfisher

New FDA draft guidance

Emphasis on connected device security:

> Software validation and risk analyses are key elements of cybersecurity analyses and demonstrating whether a connected device has a reasonable assurance of safety and effectiveness. FDA requires manufacturers to implement development processes that account for and address cybersecurity risks as part of design controls (21 CFR 820.30). For example, these processes should address the identification of security risks, the design requirements for how the risks will be controlled, and the evidence that the controls function as designed and are effective in their environment of use for ensuring adequate security.

FDA draft guidance: Device design considerations

Authenticity
(including integrity)

Authorization

Availability

Confidentiality

Secure and timely
updatability and
patchability

FDA draft guidance: Device design considerations

"...exploitation of known vulnerabilities or weak cybersecurity controls" is reasonably foreseeable and must be addressed in the design

inadequate cybersecurity controls "may cause a device to be misbranded [...] among other possible violations..."

GARDNER LAW

fieldfisher

FDA draft guidance: Premarket submission

Recommends manufacturers describe how the device design addresses and integrates these security objectives, based on...

intended use and indication	electronic data interfaces	intended/actual environment of use	types of cybersecurity vulnerabilities present	exploitability of vulnerabilities	risk of patient harm from exploited vulnerabilities

A cybersecurity risk assessment helps produce this information

For example....

D. Submission Documentation

Device cybersecurity design and documentation is expected to scale with the cybersecurity risk of that device. Manufacturers should take into account the larger system in which the device may be used. For example, a cybersecurity risk assessment performed on a simple, non-connected thermometer may conclude that the risks are limited, and therefore such a device needs only a limited security architecture (i.e., addressing only device hardware and software) and few security controls based on the technical characteristics and design of the device. However, if a thermometer is used in a safety-critical control loop, or is connected to networks or other devices, then the cybersecurity risks for the device are considered to be greater and more substantial design controls and documentation should be submitted in the premarket submission in order to demonstrate reasonable assurance of safety and effectiveness.

FDA draft guidance: Transparency

- Guidance suggests that lack of cybersecurity information provided to device users may compromise device safety and effectiveness and offers ideas about what information should be provided to users:
  - Integrating device into the use environment
  - Maintaining device cybersecurity over its lifecycle
  - Information potentially affecting safety and effectiveness of the device
- FDA also suggests that interconnected devices should include cybersecurity information in device labeling

Poll Question

Does your company have devices with cybersecurity information in the labeling?

FDA draft guidance: Security risk management

- Conduct separate safety and security risk assessments
  - Exploitability (security risk) vs. probability (safety risk)
  - Objective of security risk assessment is to ”[...] expose how threats, through vulnerabilities, can manifest patient harm and other potential risks.”
- If security risks are identified
  - Mitigate risks comprehensively in the design, or when not possible, consider compensating controls
  - If unmitigated/partially mitigated, assess them as reasonably foreseeable risks and assess for additional control measures, or risk transfer to operator/user (or even to the patient)
  - Only should rely on risk transfer if all relevant risk information is known, assessed and communicated appropriately

FDA draft guidance: Security risk management (cont.)

- Documentation
  - Summary of risk evaluation methods, processes, details of assessment and mitigation undertaken as part of risk assessment processes
  - Provides traceability between security risks, controls and the testing reports that ensure device is reasonably secure

- Total Product Life Cycle (TPLC)
  - Continue to identify, assess, and mitigate cybersecurity vulnerabilities as identified
  - Use new concept of “Secure Product Development Framework” (SPDF) throughout TPLC

Poll Question

Has your company received questions from customers about device cybersecurity?

Other cybersecurity considerations

- What are providers asking? FDA recommends that providers ask manufacturers at least these questions about medical devices:
  - How is the device updated?
  - What does it connect to?
  - What happens if the connection is unavailable?
  - What are the cybersecurity risks associated with the device?
  - What cybersecurity resources do they have to support your patients?
  - Who should you reach out to with questions if you have a concern?

Reporting medical device security concerns

- FDA does not have cybersecurity-specific reporting requirements but cybersecurity incidents can implicate MDR requirements and require reporting to FDA

- If vulnerabilities in post market devices are identified, deployment of mitigations to address cybersecurity vulnerabilities that present a risk of harm to the patient should be completed quickly

- Cybersecurity Safety Communications:
  - Example: September 2022 saw a manufacturer recall in the form of an Urgent Medical Device Correction for an insulin pump informing patients of a vulnerability and how to reduce risk.
  - https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#safety

Other cybersecurity considerations (cont.)

- HIPAA (45 CFR 160 and 164)
  - Covered entities and business associate obligations
  - Designing products to minimize PHI and support customer requirements
- Federal Trade Commission
  - Enforcement for insufficient data security controls
- State laws
  - Privacy and security requirements (e.g., CCPA, CPRA)
  - Data breach reporting/notification
- Product liability

Cybersecurity takeaways

- Design for security and address security risk management throughout the lifecycle (Secure Product Design Framework)
- Have a plan for cybersecurity vulnerabilities identified postmarket
- Plan how you will share cybersecurity risk information with FDA and device users
- Consider how cybersecurity affects device safety and effectiveness AND privacy
- Be prepared to talk with FDA about cybersecurity

State Privacy Law Comparison

State	Effective date	Access/ deletion rights	Private right of action	**PHI exclusion	Risk assess-ments	Sales opt-out	Data security standards
California	**Jan 1, 2023** (revisions)	Yes	Data breaches	Yes	Yes	Yes	Yes
Virginia	**Jan 1, 2023**	Yes	No	Yes	Yes	Yes	Yes
Colorado	Jul 1, 2023	Yes	No	Yes	Yes	Yes	Yes
Connecticut	Jul 1, 2023	Yes	No	Yes	Yes	Yes	Yes
Utah	Dec 31, 2023	Yes	No	Yes	No	Yes	Yes

GARDNER LAW

fieldfisher

Virginia Consumer Data Privacy Act (VCDPA)

- Effective **January 1, 2023**
- Applies to businesses that annually collect personal information on:
  - 100,000 VA residents; or
  - 25,000 VA residents if >50% of company revenue is from selling personal information
- Provides data subject rights, including access, correction, portability and certain opt-out rights
- Requirements include security, privacy assessments for high risk processing, transparency, contracting provisions
- Does not apply to PHI, employee, or B2B data

GARDNER LAW

fieldfisher

California Consumer Privacy Act

- California Privacy Rights Act (CPRA) changes effective **Jan. 1, 2023**:
  - **Employee/applicant and B2B data exclusions expire Jan. 1, 2023**
  - Updates to “sale” and “sharing” of personal data provision
  - Data processing with “significant risk” assessments reported to new California Privacy Protection Agency
- Enforcement trends:
  - Sephora settled in August for $1.2m resolving allegations by California attorney general that it failed to:
    - Disclose to consumers it was selling their personal information
    - Process user requests to opt-out of sales via user-enabled “global privacy controls”
  - AG has expressed intention to treat Global Privacy Control signal as “Do Not Sell My Personal Information” requests

GARDNER LAW

fieldfisher

Session Six:
EU MDR update and UK/Swiss Market Entry

Speaker:

Dr. Cord Willhöft, LL.M.
Partner, Life Sciences
cord.willhoeft@fieldfisher.com
+49 (0)172 881 49 96

Cord advises medical device manufacturers and pharmaceutical companies on matters of reimbursement eligibility, regulatory market access and healthcare compliance. His expertise includes the reimbursement and pricing of pharmaceuticals and medical devices in the stationary and outpatient service areas of the statutory health insurance (GKV).This includes practice assessment procedures before the Federal Joint Committee (G-BA) and negotiations with statutory health insurance companies and the GKV-Spitzenverband.

Cord's regulatory consulting practice particularly encompasses placing pharmaceuticals and medical devices on the market (conformity assessment procedures, authorisation, distribution, GDP, contracts between different parts of the supply chain), wholesale authorisations, compassionate use and individual imports, clinical trials and good manufacturing practice.

GARDNER LAW

fieldfisher

EU MDR Update / Swiss and UK Market Access

I. EU MDR

1. Background and DoA EU MDR
2. Transitional Periods for Notified Bodies
3. Transitional Periods for Legacy Devices / MDD-certificates
4. Legal / Political Solutions

II. Update on other Key Markets

1. UK
2. Switzerland

GARDNER LAW

fieldfisher

I. EU MDR Update (1)

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
  - 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)

- **Greatest Challenges for Manufacturers:**
  - Regulatory obligations for importer and distributors (contractual compliance)
  - MDR certificates include performance requirements (positive health impact)
  - Upgrade of SaMD
  - shortage of NBs

I. EU MDR Update (2): Notified Bodies

- **Transitional Periods for <u>Notified Bodies</u> Article 120 (1) EU MDR:**

  "*From 26 May 2021, any publication of a notification in respect of a notified body in accordance with Directives 90/385/EEC and 93/42/EEC shall become void*"

- **NBs need to obtain (new) MDR notification and – once obtained - can only grant EU DOC under MDR as of May 2021**

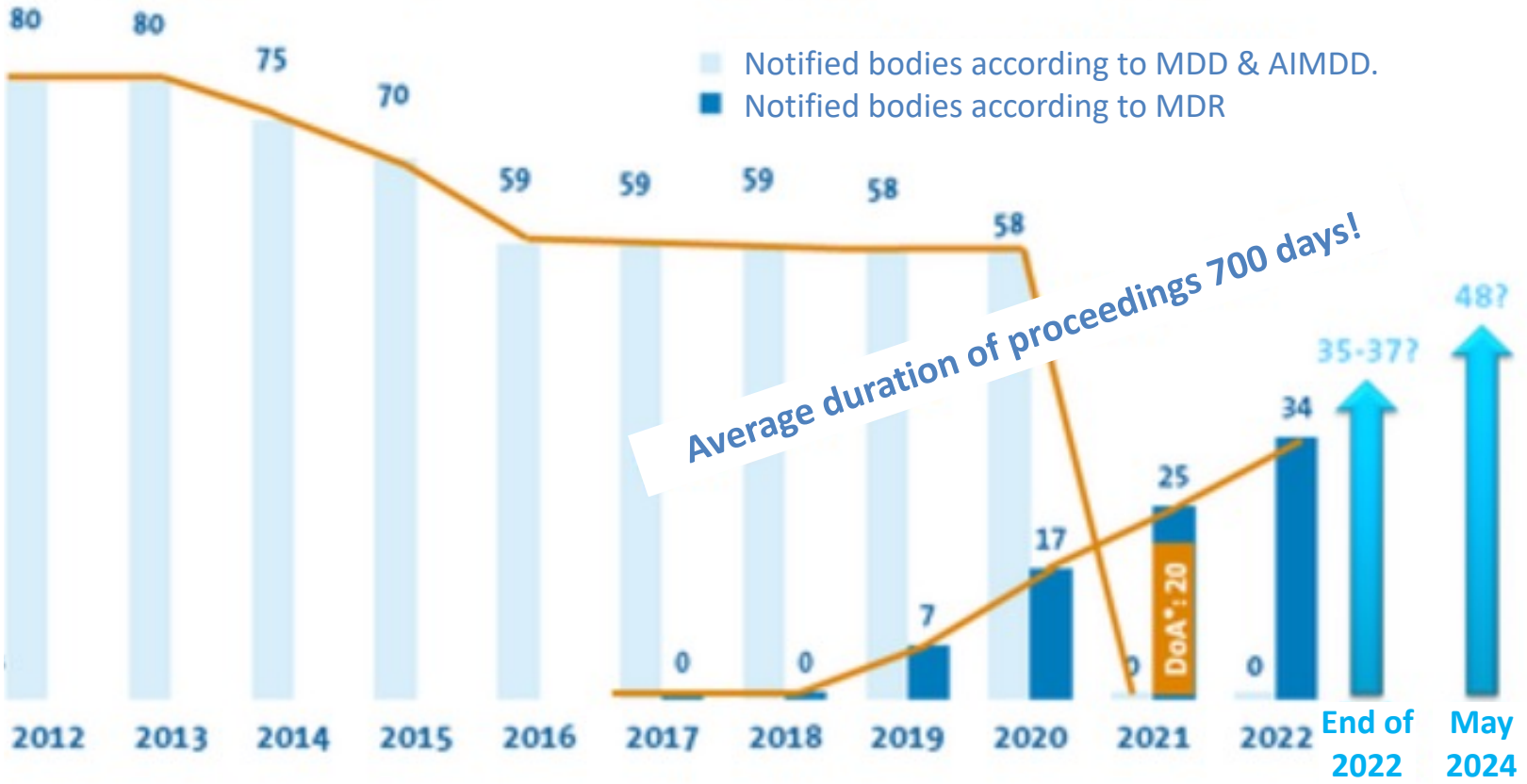
- **Consequence:** Shortage of NBs in EU and increasing competition of manufacturers for NBs

- **MDCG Guidance 2022-14:** Call to (i) apply standard fees, taking into account the interests of SME, and (ii) develop schemes in order to allocate capacities for SMEs

I. EU MDR Update (3): Notified Bodies (BVMed)

#MDReady | Number of notified bodies

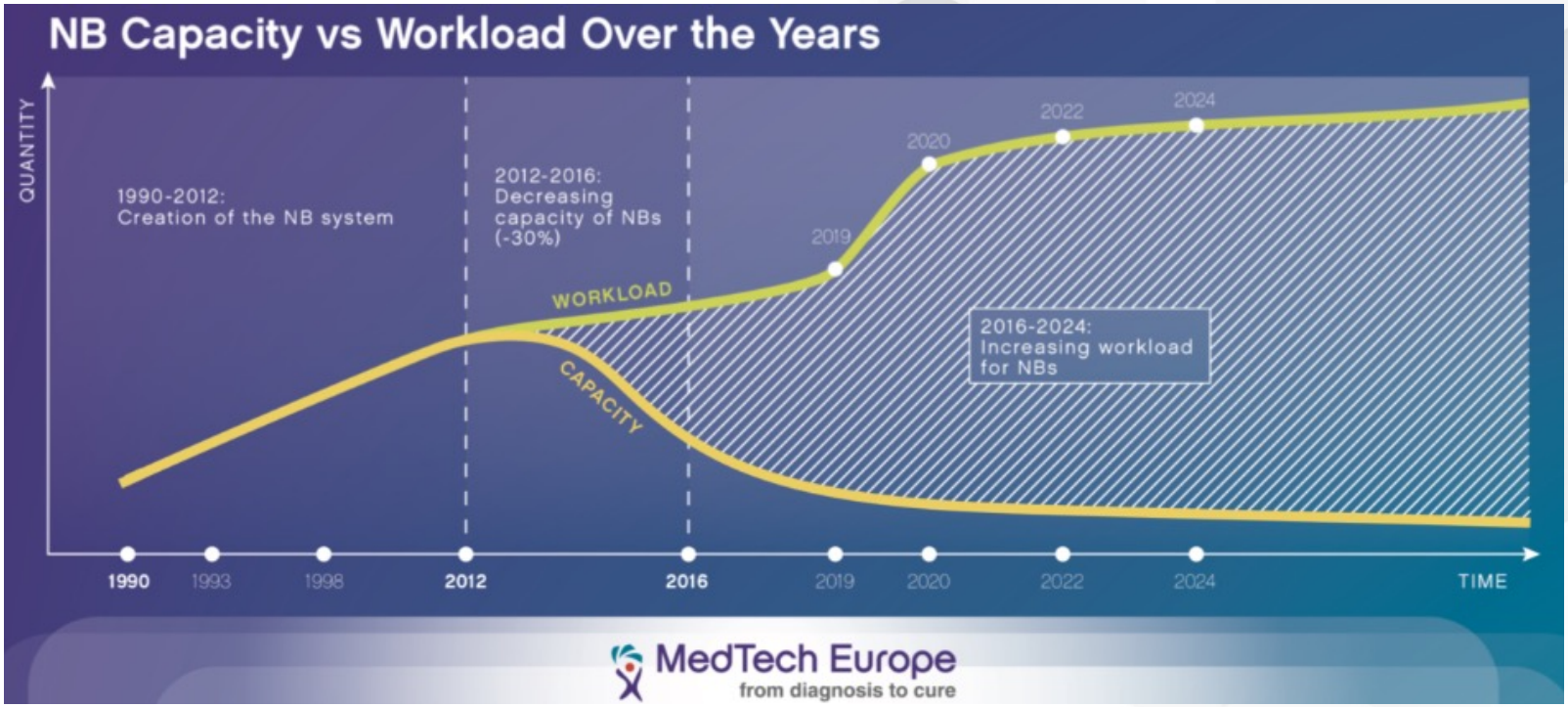
Notifications in Europe take too long. Bottlenecks are inevitable.



GARDNER LAW

fieldfisher

I. EU MDR Update (4): Notified Bodies (MedTech Europe)



GARDNER LAW

fieldfisher

I. EU MDR Update (5): Legacy Devices

- **Transitional Periods for <u>MDD certificates</u> Article 120 (3) EU MDR:**

  "*A device which (…) which has a certificate that was issued in accordance with Directive 90/385/EEC or Directive 93/42/EEC (…) may be placed on the market or put into service until 26 May 2024, provided that from 26 May 2021 it continues to comply with either of those Directives, and provided there are no significant changes in the design and intended purpose*."

  ⇒ MDD certificates remain valid until they expire, the latest until May 2024

  ⇒ 23,000 legacy devices still need to obtain MDR certificate, currently 8,120 submissions from manufacturers to NBs

  ⇒ However: 82 % of the MDR-certificates (including QMS) require 13 to 18 months, 18 % between 19 to 24 months

- **MDR Readiness of manufactures is crucial!**

I. EU MDR Update (6): Legacy Devices Solution 1

- **Short-term solution: Placing legacy devices on the market to maintain their marketability!**

  "***Devices lawfully placed on the market*** *pursuant to Directives 90/385/EEC and 93/42/EEC prior to 26 May 2021, and devices placed on the market from 26 May 2021 pursuant to paragraph 3 of this Article,* ***may continue to be made available on the market or put into service until 26 May 2025***."

- **Warehousing deadline / sell-off period until 26 May 2026, crucial to place devices on the market until their CE mark expires**

- **Commission Blue Guide (June 2022)** concerning "*placing on the market*":
  - Oral / written agreements, including contract negotiations (+)
  - physical hand-over not required (!)
  - Handing over to fulfilment service providers and released for free circulation (+)

I. EU MDR Update (7): Legacy Devices Solution 2

- **National Competent Authorities (NCA) may grant a marketing authorization for medical devices**
- **Article 59 EU MDR:** Manufacturers may apply for, and NCA may grant, a marketing authorization for (i) specific medical devices, (ii) for which the conformity assessment procedure has not been carried out, and (iii) its availability lies within the interest of public health and patient safety.
- Frequently used since 2019/2020 in Germany (BfArM)
- **Country-specific authorization** and **only for a limited period of time** (6-12 months)

GARDNER LAW

fieldfisher

I. EU MDR Update (8): Legacy Devices Solution 3

- **Political initiates from member states** (e.g German Minister of Health) **and leading Industry Associations** (SNITEM and BVMed) **in order to**
  - extend transitional period for legacy devices / CE-certificates, i.e. 2 years for class III and implantable devices, and 4 years for all other devices
  - shorten the notification procedure for NB under MDR
  - abolish the warehousing deadline / sell-off period

Note: This political initiative towards the Commission is supported by various stakeholders and also on the agenda of the next EPSCO Meeting in December

II. UK Update

- **Brexit effective as of 1 February 2020, transitional period until 31 December 2020**
- **CE-marks (MDD and MDR) are continued to be accepted in the UK until 30 June 2023**
- **Introduction of the UKCA mark** (issued by an UK Approved Body)
- **Manufacturers located outside the UK must appoint an UK-RP and must register their devices before being placed on the UK market**
- EU NB are not recognized in the UK, UK Approved Bodies may not issue CE certificates
- UK = England, Wales and Scotland. Northern Ireland accepts the EU MDR

GARDNER LAW

fieldfisher

II. Switzerland Update

- **Switzerland and the EU Commission were not able to renew the Mutual recognition Agreement until the DoA EU MDR (26 May 2021)**
- **Swiss Medical device regulation refers to EU MDR and thereby recognizes CE-Marks, no deadline**
- **However: Swiss Authorized Representative (CH-RP) must be appointed, on basis of a written mandate**

- **Identification of an importer on the labelling, packaging or accompanying documents**

GARDNER LAW

fieldfisher

Panel Discussion:
Q&A with General Counsel from Industry

Bill Revelos, JD, MS

Principal

Insight Legal Services

Alaleh Nouri, JD

EVP, Chief Legal Officer & Corporate Secretary

PROCEPT BioRobotics

Mike Pisetsky, JD, MBA

General Counsel and Chief Administrative Officer

SI - Bone

GARDNER LAW

fieldfisher