UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

In Re: COOK MEDICAL, INC., IVC FILTERS MARKETING, SALES PRACTICES AND PRODUCTS LIABILITY LITIGATION

Case No. 1:14-ml-2570-RLY-TAB
MDL No. 2570

This Document Relates to All Actions

CASE MANAGEMENT ORDER NO. 22 (QUALIFIED PATIENT DATA SECURITY AGREEMENT AND PROTECTIVE ORDER)

1. Defendants Cook Incorporated, Cook Medical LLC, *formerly known as* Cook Medical Incorporated, and William Cook Europe ApS (collectively referred to as the "Cook Defendants") and Plaintiffs (individually, a "Party" or collectively, the "Parties"), through their respective attorneys, hereby stipulate and agree to the entry of this Qualified Patient Data Security Agreement and Protective Order ("Order") in the above-captioned action.

2. This Order relates to the sharing of any patient-level data in (1) all cases transferred to this court by the Judicial Panel on the Multidistrict Litigation, including those cases identified in the original Transfer Order and those subsequently transferred as tag-along actions; and (2) all cases directly filed in or removed to this MDL.

3. This Order is intended to supplement and not replace or dilute other Orders entered in this matter to ensure compliance with the U.S. and global legal obligations for safeguarding and protecting patient-level data, including but not limited to that collected in relation to clinical trials, such as raw data[1], images, patient records and adverse event reporting

[1] Raw data refers to patient-level data that have been directly collected during a clinical trial or study (e.g. age, weight, height, medical history, images, surgery and medical treatment dates, etc. pertaining to a patient). Derived

information. As is the case with the previously entered Orders, this Order is also intended to ensure compliance with Rule 26 (c) of the Federal Rules of Civil Procedure.

4. The clinical research and data privacy (data protection) laws in the U.S., E.U. and other countries include strict requirements that are designed to protect human research subjects and the personal data about them that is collected and processed in connection with medical research.

5. Among other things, research participants must be specifically informed in writing at the outset of the research trial about the types of personal data and medical data that will be collected about them, the categories of recipients of that data, how the data will be used, whether it will be shared with others inside and outside of their country, how it will be protected, and what rights they have in relation to their data.

6. The Investigational Review Board (IRB) or Ethics Committee overseeing the research trial helps ensure (among other responsibilities) that the privacy and security obligations for research participant data are followed throughout the course of the trial. The trial sponsor, research site, and other parties entrusted with the data in relation to the research trial (e.g., experts, health authorities, safety boards, etc.) are held to strict confidentiality standards for the entire lifecycle of that data.

7. By way of example, the clinical research laws contain strict requirements and limitations on sharing or using research data for any secondary research purposes, even by the same research site, so as to protect the research subjects and minimize any use of their sensitive health data in ways that were not reasonably inferred by them when they consented to participate in the research trial. Naturally, given the strict limitations on sharing research data even within

---

data are data that is obtained from raw data and which have undergone a derivation or calculation (e.g. body mass index is derived from the weight and height of a patient).

the immediate trial and for subsequent research projects, there are even greater protections in place in relation to sharing that data third parties in other contexts, such as in the context of litigation which is not brought by the research subjects themselves.

8. Under the EU data protection laws, research participant data identified by a randomization code (i.e., so-called key-coded data) constitutes personal data, and must be protected in accordance with those laws. *See, for example, EU Data Protection Directive (95/46/EC), Chapter I, Article 2, paragraph (a)* (defining personal data as any data that directly *or indirectly* identifies a specific individual (emphasis added)); EU Data Protection Directive (95/46/EC), Recital 26 (which provides that to determine whether a person is *identifiable*, account should be taken of *all the means likely reasonably to be used either by the controller or by any other person to identify the said person*) (emphasis added)); and Article 29 Working Party Guidance Document, Opinion 4/2007 on the Concept of Personal Data, WP 136, 01248/07/EN ("The [medical device] company has construed the means for the processing, included the organizational measures and its relations with the researcher who holds the key in such a way that the identification of individuals is not only something that *may* happen, but rather as something that *must* happen under certain circumstances. The identification of patients is thus embedded in the purposes and the means of the processing. In this case, *one can conclude that such key-coded data constitutes information relating to identifiable natural persons for all parties that might be involved in the possible identification and should be subject to the rules of data protection legislation*." (emphasis added)).

9. There are similar protections for clinical research data and adverse event reports in the U.S. *See, e.g.,* the International Council of Harmonization Good Clinical Practice Guidelines (ICH GCP), E6, adopted by the U.S. Food and Drug Administration, § 4.8.10(o)

("That *records identifying the [clinical trial] subject will be kept confidential* and, to the extent permitted by the applicable laws and/or regulations, will not be made publicly available." (emphasis added)); 21 CFR § 21.70 (a)(3) (stating that clinical trial submissions submitted to the U.S. Food and Drug Administration may be disclosed to any person "*Where the names and other identifying information are first deleted, and under circumstances in which the recipient is unlikely to know the identity of the subject of the record*") (emphasis added)); 21 CFR § 20.63 (e) ("The names and any information that would identify the voluntary reporter *or any other person associated with an adverse event involving a human drug, biologic, or medical device product shall not be disclosed* by the Food and Drug Administration *or by a manufacturer* in possession of such reports in response to a request, demand, or order. Information that would identify the voluntary reporter or persons identified in the report includes, but is not limited to, the name, address, institution, or any other information that would lead to the identities of the reporter or persons identified in a report. This provision does not affect disclosure of the identities of reporters required by a Federal statute or regulation to make adverse event reports." (emphasis added)). That regulation also specifically states that the individual who is the subject of a malpractice action can obtain a copy of *his/her own report*, but that the identities *of any other individuals shall be redacted/excluded prior to disclosure*. *Id.* (emphasis added).

10. Pursuant to Case Management Order #11 (Electronically Stored Information and Document Production Protocol), Paragraph N (Clawback), and Case Management Order #7 (Agreed Qualified Protective Order Regarding Protected Health Information), Paragraph 12, this Court has outlined a process for the Parties to follow in relation to any inadvertently disclosed patient-level information.

11. Defendants have identified the risk that certain patient information could be provided inadvertently to Plaintiffs, which may contain limited patient identifiers (i.e., key-coded data).

12. As described in those Orders, the options available to Defendants include clawing back that data and redacting it before it is returned to the Plaintiffs, or allowing Plaintiffs' counsel to retain it subject to their commitment to protect the data in a manner commensurate with applicable laws and requirements.

13. To ensure compliance with applicable clinical research and data protection laws while arriving at a practical approach that does not unduly burden the Court or the Parties, the Parties have agreed that Plaintiffs' counsel may retain any key-coded data that may have already been provided subject to the following protections:

a. Plaintiffs' counsel will take steps to ensure that the key-coded data which was provided by the Defendants is only accessible on a 'least privilege' basis to attorneys, paralegals and other staff members of their firms that are working on this matter, and not any other firm attorneys, employees or consultants who may otherwise have access to the firm(s) file room and electronic systems in which matters are stored.

b. Plaintiffs' counsel will ensure that those individuals entrusted with the data within its firm(s) are aware of this Order and the required security obligations that apply to the key-coded data. They also confirm that they will obtain written assurances from any subcontractors entrusted with the data (such as experts, IT security support, temporary personnel, etc.) that they understand the security requirements

applicable to the data as described in this Order, and agree to uphold an equivalent level of protection for the key-coded data. See attached Exhibit A.

c. Plaintiffs' counsel confirms that it will safeguard the key-coded data throughout its lifecycle, in a manner commensurate with its sensitivity. This includes, for example, not storing the data on any mobile device or disk unless the device or disk is encrypted, only transmitting the data via secure, encrypted channels (such as secure file transfer protocols) and not via email, and ensuring that any hard copies of the data are sent via federal express or other secure means to minimize any unauthorized access.

d. Plaintiffs' counsel will ensure that all electronic storage locations for the data, including back-ups, contain security safeguards that ensure an adequate level of protection for the data, including up-to-date anti-virus protection, industry-standard password management practices, and automatic log-outs after 15 minutes of inactivity.

e. Plaintiffs' counsel will ensure that the data is only copied when necessary for purposes of the litigation, and that all copies are safeguarded in a consistent manner to that described in this Order.

f. Plaintiffs' counsel will ensure that disposal of the key-coded data takes place in a secure manner, such as by shredding, pulverizing or irreversibly destroying hard copies of the data, and by erasing electronic copies using industry standards (such as those issued by the National Institute for Standards and Technology).

g. Plaintiffs' counsel confirms that it will not attempt in any way to re-identify or contact, directly or indirectly through contractors or vendors, any of the

individuals whose data has been provided to it, and that doing so is in direct violation of this Order.

h. Plaintiffs' counsel also confirms that it will not share any of the data with any unrelated parties to this MDL, whether in the context of litigation or otherwise, and that doing so is in direct violation of this Order.

i. Plaintiffs' counsel confirms that it will limit the retention of the data to a period of three (3) years following the conclusion of this litigation (including any appeals that may take place), and will then take steps to irreversibly destroy/erase the data as outlined in this Order. Plaintiffs' counsel agrees to sign a Certificate of Destruction to that effect within 90 days after the three-year retention period has expired.

j. Plaintiffs' counsel recognizes and agrees that it is responsible for any violation of these security requirements contained in this Order by any employee of its firm as well as by any of its subcontractors or other agents that it retains and entrusts with the data.

k. Should Plaintiffs' counsel become aware of any security incidents involving this data, which subject the data to unauthorized access, loss, misuse or alteration, they will inform Defendants within three (3) business days of identifying such situation, and cooperate fully with Defendants in relation to any legal obligations that may arise in relation to that situation, such as in relation to applicable breach notification laws.

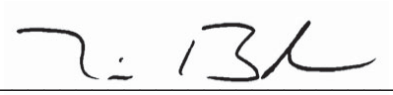
l. The Parties will also take reasonable steps to protect the data from any unnecessary disclosure in relation to any depositions that take place in relation to this matter.

14. The Parties understand and agree that this Order does not affect the ongoing responsibilities of the Parties to redact any other medical data produced in this matter or to comply with other Orders entered by the Court in relation to the protections of that data.

15. This Order survives the conclusion of this litigation.

IT IS SO ORDERED.

Date: 7/14/2017



Tim A. Baker
United States Magistrate Judge
Southern District of Indiana

AGREED TO BY:

/s/ Joseph N. Williams
Joseph N. Williams
Riley Williams & Piatt LLC
301 Massachusetts Avenue
Indianapolis, IN 46204
Tel: (317) 633-5270
Fax: (317) 426-3348
jwilliams@rwp-law.com

Michael W. Heaviside
HEAVISIDE REED ZAIC
312 Broadway, Suite 203
Laguna Beach, CA 92651
Tel: (949)715-5120
Fax: (949)715-5123
mheaviside@hrzlaw.com

Ben C. Martin
LAW OFFICE OF BEN C. MARTIN
3219 McKinney Ave., Ste. 100
Dallas, TX 75204
Tel: (214) 761-6614
Fax: (314) 744-7590
bmartin@bencmartin.com

David P. Matthews
MATTHEWS & ASSOCIATES
2905 Sackett St.
Houston, TX 77098
Tel: (713) 522-5250
Fax: (713) 535-7136
dmatthews@thematthewslawfirm.com

Counsel for Plaintiffs

/s/ Andrew L. Campbell
Andrea Roberts Pierson
Andrew L. Campbell
John T. Schlafer
FAEGRE BAKER DANIELS LLP
300 North Meridian Street, Suite 2700
Indianapolis, Indiana 46204
Tel: (317) 237-0300
Fax: (317) 237-1000
E-Mail: andrea.pierson@faegrebd.com
E-mail: andrew.campbell@faegrebd.com
E-Mail: john.schlafer@faegrebd.com

Counsel for the Cook Defendants