IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISRICT OF INDIANA
INDIANAPOLIS DIVISION

IN RE: COOK MEDICAL, INC., IVC
FILTERS MARKETING, SALES
PRACTICES AND PRODUCT LIABILITY
LITIGATION

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

This Document Relates to All Actions

CASE MANAGMENT ORDER #11
(ELECTRONICALLY STORED INFORMATION AND DOCUMENT PRODUCTION
PROTOCOL)

This Order shall govern: (1) all cases transferred to this court by the Judicial Panel on

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. It is ORDERED as follows:

A. Scope

1.   General. The procedures and protocols outlines herein govern the production of

electronically stored information ("ESI") and paper documents by the Parties during the

pendency of this litigation. The production formats for any other materials will be addressed by

the Parties after a meet and confer regarding specific item or category of items. Nothing in this

protocol will be interpreted to require disclosures of documents or information protected from

disclosure by the attorney-client privilege. The Parties agree that issues related to the

application of Danish and/or European Union law regarding data privacy will be the subject of a

separate order based on the Parties' separate briefing.

2.   <u>Limitations and Non-Waiver</u>. This protocol provides a general framework for the production of ESI and paper documents on a going forward basis. The Parties and their attorneys do not intend by this protocol to waive their rights to the work-product doctrine or any applicable privilege, and it shall not extend to other matters or information not specifically described herein. All Parties preserve their attorney-client privileges and other privileges and there in no intent by the protocol, or the production of documents pursuant to the protocol, to in any way waive or weaken these privileges.

B. ESI Preservation

1.   The Parties issued litigation hold notices to those persons identified as most likely to have discoverable information, including, but not limited so, all those persons disclosed to date pursuant to Fed. R. Civ. P. 26 and any action transferred to this MDL, the custodians identified by plaintiffs' counsel, custodians identified by defense counsel, the persons identified in the ESI Order entered in the <u>Adams v. Cook Medical, et al,</u> USDC (SD Ind) Case No: 1:13-cv-00013, those persons identified within this Order and any other person within the scope of Fed. R. Civ. P. 26(a)(1)(A).

2.   All reasonably identifiable processes and procedures which would result in the elimination, or transfer to a less accessible medium, of any unpreserved data and associated metadata which would otherwise be required to be preserved or produced have been suspended by the Parties. This does not imply the Parties have an obligation to preserve data and associated metadata which is greater than what the Federal Rules of Civil Procedure require.

3.   Custodians: For each Custodian identified as set forth above and in Section D below or subsequently:

a. The hard drives of such Custodian have been or, in the case of subsequently identified custodians, will be, preserved by the creation of a full forensic, bit-for-bit image of any computer where relevant work was performed by such Custodian. Each such image preserves both the active file spaces of the target computer, as well as the unallocated file spaces, including file system metadata. In cases where Custodians possess unusually large personal hard drives coupled with small and/or less relevant data sets, the logical files will be collected in a forensically sound manner, avoiding the undue burden of creating a full (bit-by-bit) forensic image.

b. The personal or network storage areas for each such Custodian have been or, in the case of subsequently identified Custodians, will be, preserved in whole.

c. The entire email box for each Custodian has been forensically or, in the case of subsequently identified Custodians, will be, preserved in whole, including all folder structures and the trash bins.

d. Removable media, including PDA/Smart Phones, will be collected, preserved and processed when responsive information not contained on another collected source is identified by the Custodian.

e. The Parties understand and will meet the preservation obligations they have under the Federal Rules of Civil Procedure.

C. Sources

1. The following are Defendants' data sources identified to date that are most likely to contain relevant information:

User-Generated Document Sources

Microsoft Exchange Servers in Denmark, Bloomington, Indiana and West Lafayette, Indiana

File Servers in Denmark, Bloomington, Indiana and West Lafayette, Indiana

Web Office in Bloomington, Indiana

Databases, System-Generated ESI Sources, and Other Structured Data

Livelink in Denmark, Bloomington, Indiana and West Lafayette, Indiana

Trackwise Database in Bloomington, Indiana

Coursemill Training Databases in Bloomington, Indiana

Digital Asset Management Database in Bloomington, Indiana

PDM Link in the U.S.

Marketing Project Tracker

Regulatory Project Tracker

Engineering Project Tracker

JBase Database in Denmark and Bloomington, Indiana

Navision System in Denmark and Bloomington, Indiana

Business Objects

2.   ESI reasonably identified from these areas will be preserved consistent with

Defendants' obligations under the Federal Rules of Civil Procedure.

3.   Defendants understand their continuing obligations under the Federal Rules of

Civil Procedure regarding subsequently identified databases, document stores, repositories and

application data.

D. **Custodians**

1.   The following are "Key" Defense Custodians who have been identified by Defendants to date as most likely to have information discoverable to this litigation. For these Custodians, data is being preserved from e-mail systems, computer systems, relevant removable storage media, and physical files that are in the possession, custody, and control of Defendants. These Key Defense Custodians include: Darrell Talbert, Mark Frey, Molly Busenbark, Brian Choules, Tony Ragheb, Jennifer Brown, Mark Breedlove, Rob Lyles, Arne Mølgaard-Nielsen, Camilla Wamberg Munkesoe, Annette Lüneborg, Henrik Gyllun, Per Hendriksen, Anna Bjerg Jessen, Torben Andersen, Mette Neiendam Nielsen and Bruce Fleck.

2.   The parties understand their continuing obligations under the Federal Rules of Civil Procedure to identify Custodians whom they believe are reasonably likely to have discoverable information and will hand the custodians' ESI consistent with those obligations.

E. **Departmental / Project / Collaboration / Shared Storage Spaces:**

1.   The following are departmental / project / collaboration / shared storages areas of the Defendants which have been identified to date as likely to have information relevant to this litigation. Potentially relevant ESI from these areas will be preserved pending identification of data to be produced into this litigation.

Document File Servers in Denmark, Bloomington, Indiana and West Lafayette, Indiana.

2.   Defendants understand their continuing obligations under the Federal Rules of Civil Procedure to disclose the identity of other document file servers that Defendants subsequently identify as being reasonably likely to contain information responsive to discovery requests.

F. ESI and Record Retention Policies

1.   Defendants have identified all ESI and Record Retention Policies and Procedures, including those pertaining to back-up and/or disaster recovery systems and associated policies, processes and procedures, including those related to the deletion or removal of data. To the extent that additional ESI and Record Retention Policies and Procedures are discovered by Defendants, they will identify them consistent with their obligations under Fed. R. Civ. P. 26(e).

G. ESI Search

1.   To the extent that there are any disagreements regarding search methodology and implementation that have not already been resolved by this Court, the parties shall bring those matters to this Court's attention.

2.   The Parties agree that Defendants will search User-Generated files, after de-nisting and deduplication, to identify a set of potentially relevant documents for review by Defendants. Furthermore, the Parties agree to exclude the following types from the search and review:

BINARY

BINHEXENCODEDTEXT

BITMAPBEGIN

[BLANK]

EPSTIFF

EXECUTABLE

FFT

FLASH6

FLASH9

IGES

JAVACLASS

PARADOX4

POSTSCRIPT

TNEF

VCAL

WIN COMPILEDHELP

WIN SHORTCUT

WINDOWSICON

H. **Electronically Stored Information**

1.   The Parties agree that User-Generated and System-Generated Document Sources (see above,) are being produced for the primary purpose of responding to discovery requests. The Parties shall meet and confer to work out any issues concerning production and access to System-Generated Document Sources where it is claimed will place an unreasonable burden on Cook's ongoing business and/or IT operations.

2.   <u>User-Generated Document Sources</u>: The Parties will produce the following User-Generated Document Sources in "Native Format" (with accompanying placeholder TIFFs as described in paragraph 2.d), and provide a load file of extracted metadata and OCR/full text: (1) spreadsheets (.xls files); (2) PowerPoint presentations (.ppt files); (3) Word documents; (4) audio and video formats such as mp3s, wavs, megs. All other User-Generated Document Sources, except as described in paragraph 3 (System-Generated Document Sources), will be produced as TIFFs, created data and extracted metadata and text.

a.   Natives: "Native Format" as referenced Paragraph 2 above is defined as document files in the file format in which the item was collected with internal and system metadata intact. For example, the native format of a Microsoft Office WORD document is as a .doc or .docx file. Native files will be produced in their complete original condition, and may not be altered in any way for litigation purposes, except as noted herein related to redactions.

b.   Load Files: The load files will include an image load file in Opticon or IPRO format as well as a data (.DAT) file with the created data and metadata fields identified in Exhibit A on the document level to the extent available. The producing party shall also identify for each document, the request(s) (by set and number) to which the document is responsive at the time the document is produced or provide the filepath which shows how the document is maintained in the ordinary course of business.

c.   ESI Processing Dates: All documents shall be produced so as to show the metadata date in Eastern Standard Time. Reasonable efforts will be made to display all the dates displayed in documents being TIFF'ed, e.g., emails, in Eastern Standard Time.

d.   Production of TIFF's for Native Format Documents that are Impractical to Convert to TIFF: The following ESI types do not lend themselves well to the TIFF format: spreadsheets (.xls files); PowerPoint presentations (.ppt files); audio and video formats such as mp3s, wavs, megs. A Bates-stamped placeholder TIFF, bearing the legend "This document has been produced in native format" shall be produced for such documents; these placeholders will be Bates Numbered in the same way as any other TIFF and the Bates Number of that single page shall be used as the BEGINBATES and ENDBATES of the associated document.

3.   System-Generated Document Sources: Only the portions of a database that are responsive to requests will be produced (as tabular data, e.g., as database, CSV or Excel

files, including all associated fields, and, when the database includes documents, as native files with database and system metadata intact). Databases that are entirely responsive will be produced in their entirety. Defendants have provided a list of Cook System-Generated Document Sources, which integrate databases and data stores in a structurally complex way. The Parties will make reasonable efforts to preserve, identify, collect, process/assemble, review and produce responsive information based on specific requests for document production. After review, if the requesting party believes that any of these types of sources contain additional responsive ESI is in this category, counsel should initiate a meet and confer to address production issues and additional data or means to provide data can be provided. Reasonable effort will be made by the producing party to provide the ESI as close as possible to its database form, including native files that are generated by or easily made a part of the system. These documents will be produced accompanied with a Bates number and MD-5 hash value.

4.   The load files will include an image load file in Opticon or IPRO format as well as a data (.DAT) file with the created data and metadata fields identified in Exhibit A on the document level to the extent available. The producing party shall also identify for each document the request(s) (by set and number) to which the document is responsive at the time the document is produced or provide the filepath which shows how the document is maintained in the ordinary course of business.

I.   **Documents That Exist Only in Paper Format**

1.   Documents that only exist in paper form shall be scanned and produced as TIFF's with the same load files and metadata fields as provided for ESI, to the extent that said metadata exists, along with OCR'ed text.

2.   Unitization: Unitization and the parent/child relationships of such documents shall be preserved and provided in the load files, for newly scanned documents and, to the extent that it exists, for previously existing scanned image sets (for example, hard copy documents scanned prior to the commencement of the litigation that no longer exist in hard copy will be produced with "as is" unitization).

3.   Metadata: To the extent that it is available to or has been derived by the producing party, the producing party shall provide metadata (or objective coding to the extent it already exists) for such documents in accordance with paragraph H.4.above. At a minimum, the production load file should include custodian information, the document's redaction status, and the document's confidentiality status.

4.   OCR: Industry standard multipage OCR text shall be provided for each paper document. Page breaks shall be preserved within the OCR text. OCR text files shall match the respective bates number of its documents, with a file extension of "txt."

J. Additional Production Specification:

1.   TIFFs: All TIFFs produced by any party in this matter will be single page Group IV TIFF format, 300 dpi quality or better.   Image file names will be identical to the corresponding bates numbered images, with a ".tif" file extension. TIFF versions of ESI produced pursuant to this section shall include visible and legible images of comments and hidden text contained within the underlying ESI.

2.   Bates Numbers:

a.   All bates numbers will consist of an Alpha Prefix, followed immediately by an 8 digit numeric: [alpha prefix]########. There must be no spaces in the bates number. Any numbers with less than 8 digits will be front padded with zeros to reach the required 8 digits.

b.   The producing party will brand all TIFF images in the lower right-hand corner with its corresponding bates number, using a consistent font type and size. The Bates number must not obscure any part of the underlying image. If the placement in the lower right-hand corner will result in obscuring the underlying image, the Bates number should be placed as near to that position as possible while preserving the underlying image.

3.   Confidentiality Treatment: The Parties anticipate agreement to one or more Protective Orders in this matter, which will specify various confidentiality treatment levels for use in this matter for documents and data produced.

a.   The confidentiality treatment level for any item will be provided with the review created data provided by the Producing Party for that item, in the field entitled "Confidentiality". For items with no confidentiality requirements, the field will be left blank.

b.   The producing party will brand any confidentiality endorsements in a corner of any TIFF images representing the produced item. Those endorsements must be in a consistent font type and size, and must not obscure any part of the underlying image or Bates number.

4. Redaction:

a. No agreement has been reached between the Parties concerning redaction of non-privileged information that is deemed non-responsive within a document that also contains

responsive information. The Parties will meet and confer to resolve any disputed redaction. In the event that the Parties are unable to agree about a redaction, the Party seeking to redact a portion of the otherwise responsive document, shall within five days of any notice of dispute to arrange the Court's assistance to resolve the dispute via a telephone conference and/or hearing with the Magistrate and shall provide the Magistrate with an unredacted version of the document for an in camera review prior to the conference or hearing. Nothing in this paragraph shall prevent either Party from moving to compel production of all responsive documents without redaction or seeking protective order allowing redaction of the portions of all responsive documents that reference non-responsive matters.

b. All items redacted for privilege, whether paper documents or ESI, will be produced as TIFFs unless they are structured data produced in tabular format. No native ESI items will be produced for redacted items. However, to the extent that the text is searchable in the native format, the producing party must provide searchable text for those portions of the document that have not been redacted.

c. The TIFF and/or underlying metadata for a redacted item will bear labels identifying the area of each redaction and the basis for the redaction.

d. For redacted items which were originally ESI, all unredacted metadata fields will be provided and will include all non-redacted data.

e. Redacted documents shall be identified as such in the load file provided with the production. A document's status as redacted does not relieve the producing party from providing all of the metadata required herein.

5.   De-duplication: De-duplication will occur to promote efficiencies in the collection and review process.   Copies of a document with the same MD5 hash values need be

produced only once, provided that any document which is part of a document family (i.e., has the same BEGATTACH and ENDATTACH) which includes a produced document will not be withheld as a duplicate. Email MD5 hash values will be calculated for entire mail families, including attachments. The CaseDataTM fields that will be used to create MD5 hash value for an email include:

a.   MAPPED_RECIPIENTS.   MD5 Hash performed on coalesce of: mail_to; to; sendto; displayto; recipientsdisplay.

b.   MAPPED_CC.   MD5 Hash performed on coalesce of: mail_cc; cc; copyto; displaycc.

c.   MAPPED_BCC.   MD5 Hash performed on coalesce of: mail_bcc; bcc; blindcopyto.

d.   MAPPED_AUTHOR.   MD5 Hash performed on coalesce of: mail-_creator_name; mail_from; from; primaryauthor; author; lastsaveby; mail_last_modifier_name; chair; last_saved_by; sendername.

e.   MAPPED_AUTHOREMAIL.   MD5 Hash performed on coalesce of: mail_sender_email_address; from; senderemailaddress.

f.   MAPPED_SUBJECT.   MD5 Hash performed on coalesce of: mail_subject; subject; normalizedsubject.

g.   MAPPED_SENTDATE. MD5 Hash performed on coalesce of: Deliverdate; Posteddate;   Sent;   Senton;   mail_client_submit_time;   client_submit_time;   clientsubmittime; deliverytime.

Emails will be de-duplicated at a family level, with the MD5 hash values for a family being calculated on the concatenated MD5 hash values of an email and all its attachments. With each

production, Defendants will provide a de-duplication report, as an Excel or Concordance .dat overlay file, listing the custodian, file path or email folder for each document withheld as a duplicate as well as the Bates number of the produced document of which it is a duplicate.

6.   Color: Paper Documents and ESI reduced to TIFF shall be produced in black and white in the first instance. If a paper document or redacted ESI contains color and that color is necessary to decipher the meaning, context, or content of the document, the producing party shall honor reasonable requests for either the production of the original document for inspection and copying or production of a color image of the document.

7.   Load Files: The load file format for productions shall be in .dat format.

8.   Encrypted or Password Protected ESI: For any ESI that exists in encrypted format or is password-protected, the producing party will provide the receiving party a means to gain access to those native files (for example, by supplying passwords.) If the password cannot be found through reasonable efforts, the Parties will meet and confer to determine a process for handling password protected documents.

9.   Production Media: The Parties will use the appropriate electronic media (CD, DVD or hard drive) for ESI production, and will cooperate in good faith to use the highest-capacity available media to minimize associated overhead. The producing party will label the physical media with the producing party, production date, media volume name, and document number range. Any replacement Production Media will cross-reference the original Production Media, clearly identify that it is a replacement and cross-reference the Bates Number range that is being replaced.

10.   Metadata in Extracted Text: Defendants agree to insert the "To, From, DATERCVD" fields extracted from the metadata for emails into the Extracted Text field for all email documents.

K. Timing

1.   The Parties will comply with the Court's discovery schedule and the Federal Rules of Civil Procedure.

2.   The Parties will produce ESI on a rolling basis.

L. General Provisions

1.   Any practice or procedure set forth herein may be varied by agreement of the Parties, and first will be confirmed in writing, where such variance is deemed appropriate to facilitate the timely and economical exchange of electronic date.

2.   Should any party subsequently determine is cannot in good faith proceed as required by this protocol, the Parties will meet and confer to resolve any dispute before seeking Court intervention.

3.   The Parties agree that e-discovery will be conducted in phases and the Parties will meet and confer regarding discovery of data sources not listed herein.

4.   Regardless of the foregoing, the Parties, subject to objections asserted pursuant to the Federal Rule of Civil Procedure, retain the obligation to produce all responsive non-privileged documents of which they are aware.

5.   By entering into this protocol, the Parties do not waive any of their respective rights under the Federal Rules of Civil Procedure.

M. Documents Protected From Discovery

1.   Pursuant to Fed. R. Evid. 502(d), the production of a privileged or work-product protected document, whether inadvertent or otherwise, is not a waiver of privilege or protection from discovery in this case or in any other federal or state proceeding. For example, the mere production of privileged or work-product-protected documents in this case as part of a mass production is not itself a waiver in this case or in any other federal or state proceeding.

2.   Responsive documents withheld from production based on a claim of privilege shall be reflected on a privilege log consistent with the Protocol Concerning Claims of Privilege and Work Product.

N. Clawback

1.   The Parties acknowledge the requirements of the Federal Rule of Civil Procedure 26(b)(5)(B) in the event of the inadvertent production of documents, files or information subject to the protection of any applicable privilege or the work product doctrine. The Parties agree to specifically extend this clawback procedure to also include any inadvertent production of documents, files or information subject to data privacy laws of Denmark and/or the European Union.

SO ORDERED: 7/10/2015

_____

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

AGREED TO BY:

s/ Ben C. Martin (with consent)	*s/ Christopher D. Lee*
Ben C. Martin	Douglas B. King, Esq.
LAW OFFICE OF BEN C. MARTIN	James M. Boyers, Esq.
3219 McKinney Ave., Ste, 100	Christopher D. Lee, Esq.
Dallas, TX 75204	John C. Babione, Esq.
Tel: (214) 761-6614	Sandra L. Davis, Esq.
Fax: (314) 744-7590	Kip S. M. McDonald, Esq.
bmartin@bencmartin.com	WOODEN & McLAUGHLIN LLP
	One Indiana Square, Suite 1800
Michael W. Heaviside	Indianapolis, IN 46204-4208
HEAVISIDE REED ZAIC	Tel: (317) 639-6151
312 Broadway, Suite 203	Fax: (317) 639-6444
Laguna Beach, CA 9265	dking@woodmclaw.com
Tel: (949)715-5120	jboyers@woodmclaw.com
Fax: (949)715-5123 mheaviside@hrzlaw.com	clee@woodmclaw.com
	sdavis@woodmclaw.com
David P. Matthews	kmcdonald@woodmclaw.com
MATTHEWS & ASSOCIATES	
2905 Sackett St.	Counsel for Cook Defendants
Houston, TX 77098	
Tel: (7130 522-5250	
Fax: (713) 535-7136	
dmatthews@thematthewslawfirm.com	
Lead Co-Counsel for Plaintiffs	

Copies to all registered counsel of record
via the Court's ECF system.

All non-registered counsel of record will be
served by Plaintiffs' Lead Counsel.

EXHIBIT A

Field	Definition	Doc Type
SOURCE	Name of party producing the documents	All
CUSTODIAN	Name of person or other data source (non-human) from where documents/files are produced. *Where redundant names occur, individuals should be distinguished by an initial which is kept constant throughout productions (e.g., Smith, John A. and Smith, John B.)*	All
BEGBATES	Beginning Bates Number (production number)	All
ENDBATES	End Bates Number (production number)	All
PG COUNT	Number of pages in the document	All
FILESIZE	File size of either the original or expanded/uncompressed file	All
APPLICAT	Commonly associated application category for the specified file type.	All
FILEPATH	Original file/path location where the item was located at the time of collection. This should include location, file name, and file extension.	E-document
NATIVEFILELINK	For documents provided in native format only	All
TEXTPATH	File path for OCR or Extracted Text Files	All
MSGID	Email system identifier assigned by the host email system. This value is extracted from the parent message during processing	E-mail
PST/OST filename	PST/OST filename.	E-Mail
Folder	Folder location of the e-mail within the PST/OST. Mailbox or file	E-Mail
FROM	Sender	E-Mail

TO	Recipient	E-Mail
CC	Additional Recipients	E-Mail
BCC	Blind Additional Recipients	E-Mail
SUBJECT	Subject line of e-mail	E-Mail
CONVERSATIONINDEX	Email Thread Identification	E-Mail
ATTACHBATES	Bates number from the first page of each attachment	E-Mail
BEGATTACH	First Bates number of family range (i.e. Bates number of the first page of the parent e-mail)	E-Mail
ENDATTACH	Last Bates number of family range (i.e. Bates number of the last page of the last attachment)	E-Mail
ATTACHCOUNT	Number of attachments to email	E-Mail
ATTACHNAMES	Names of each individual Attachment, separated by semi-colons	E-Mail
DATESENT (mm/dd/yyyy hh:mm:ss AM)	Date Sent	E-Mail
DATERCVD (mm/dd/yyyy hh:mm:ss AM)	Date Received	E-Mail
E-Mail Outlook Type	Type of Outlook item, e.g., e-mail, calendar item, contact, note, task	Outlook or similar system
HASHVALUE	MD5 hash value	All
TITLE	Title provided by user within the document	E-document
AUTHOR	Creator of a document	E-document
DATECRTD (mrn/dd/yyyy) hh:mm:ss AM)	Creation Date	E-document

FSDATECRTD	File system date created	E-document
LAST MODIFIED BY	Last person who modified (saved) a document	E-document
LASTMODD (mrn/dd/yyyy hh:mm:ss AM)	Last Modified Date	E-document
FSLASTMODD	File system date modified	E-document
Document Type	Descriptor for the type of document: "**E-document**" for electronic documents not attached to e-mails; "**E-mail**" for all e-mails; "**E-attachment**" for files that were attachments to e-mails ; and "**Physical**" for hard copy physical documents that have been scanned and converted to an electronic image.	All
Importance	High importance – indicates Priority E-mail message	E-mail
Redacted	Descriptor for documents that have been redacted. "Yes" for redacted documents; "No" for un-redacted documents.	All
RedactionReason	Basis of redaction. If more than one, separate reasons by semi-colons	All
ProdVol	Name of media that data was produced on.	
Confidentiality	Confidentiality level if assigned pursuant to any applicable Protective Order stipulation.	All

20