

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

IN RE: INVOKANA (CANAGLIFLOZIN)	:	MDL NO. 2750
PRODUCTS LIABILITY LITIGATION	:	3:16-md-2750 (BRM)(LHG)
	:	
	:	JUDGE BRIAN R. MARTINOTTI
	:	JUDGE LOIS H. GOODMAN
	:	

**CASE MANAGEMENT ORDER NO. 16
(ORDER REGARDING ELECTRONICALLY STORED INFORMATION)**

The Parties hereby agree to the following protocol for production of electronically stored information (“ESI”) and paper (“hardcopy”) documents. Subject to protective orders in this Action, this protocol governs all production in the matter. Nothing in this protocol shall limit a party’s right to seek or object to discovery as set out in applicable rules, to rely on any protective order entered in this action concerning protection of confidential or otherwise sensitive information, or to object to the authenticity or admissibility of any hardcopy document or ESI produced in accordance with this protocol.

A. GENERAL AGREEMENTS

1. Ongoing Cooperation among the Parties

The parties are aware of the importance the Court places on cooperation and commit to continue to consult and cooperate reasonably as discovery proceeds.

2. Proportionality

- a. Discoverable Custodians and Non-Custodial Data Sources. Consistent with the proportionality standard, within 45 days after entry of this Protocol, each Party shall provide to other Parties a list of the Party’s most likely custodians, as well as a list of non-custodial data repositories, whose reasonably accessible emails and other ESI will be searched for relevant information. Custodians shall be identified by name, title, dates of employment by the Party, and a brief description of employment duties. If any custodian or data source identified in the paragraph is located outside the United States, the Parties shall meet and confer regarding such matters as relevancy and privacy of the data at issue and, as applicable, the timing of production of any such data.

- b. On-Site Inspections of ESI. On-site inspections of ESI under Rule 34(b) shall be permitted only upon a good-faith showing by the Requesting Party of good cause and specific need or upon agreement of the parties. As appropriate, the Court may condition on-site inspections of ESI, as authorized in the preceding sentence, to be performed by independent third-party experts, and the Court may set other conditions deemed appropriate by the Court.
- c. Non-Discoverable ESI. Absent a Party's specific written notice for good cause, the following categories of ESI are presumed to be inaccessible and not discoverable:
- i. ESI deleted in the normal course of business before the time a preservation obligation in this matter came into effect;
 - ii. Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including (but not limited to) backup tapes, disks, SAN, and other forms of media, and that are substantially duplicative of data that are more accessible elsewhere;
 - iii. Deleted, "slack," fragmented, or unallocated data only accessible by forensics;
 - iv. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;
 - v. On-line access data such as (without limitation) temporary internet files, history files, cache files, and cookies;
 - vi. Data in metadata fields frequently updated automatically, such as last-opened or last-printed dates;
 - vii. Electronic data (e.g., call logs, email, calendars, contact data, notes, and text messages) sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices), provided that a copy of all such electronic data is routinely saved elsewhere (such as on a server, laptop, desktop computer, or 'cloud' storage);
 - viii. Voicemail, including Telephone or VOIP voice messages unless the Voicemail was of mass distribution;
 - ix. Text messages that are not retained in the ordinary course of business;
 - x. Instant messages that are not substantively related to the products at issue in this matter and that are not retained in the ordinary course of business;
 - xi. Server, system, network, or software application logs;
 - xii. Data remaining from systems no longer in use that is unintelligible on the systems in use;
 - xiii. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report.
 - xiv. Structural files not material to individual file contents that do not contain substantive content (e.g. .CSS, .XSL, .XML, .DTD, etc.).
- d. The Parties agree that individuals that may be in possession of data referenced in sections A.2.c.vii, viii, ix, and x, above, over which a Party has custody, possession, and control, and which may contain relevant information, have been made aware of their obligations to preserve relevant information and were provided with preservation instructions.

- e. Disaster-Recovery Backup Data. Absent a Party's specific written notice for good cause, no Party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes. Absent a showing of good cause, such backup media shall be considered to be not reasonably accessible.

3. No Designation of Discovery Requests

The Producing Party shall identify the key source(s) of ESI that contain non-duplicative responsive documents (e.g., custodial files or database productions). Any custodial files or database productions will be produced with an index, in native excel spreadsheet format, identifying the bates range of each production that corresponds to each custodian or database. Productions of hardcopy documents and ESI in the reasonably usable form set out in this protocol, including Attachment A, otherwise need not be organized and labeled to correspond discovery requests. However, the Requesting Party may make reasonable requests for identification by bates number of groups of documents that the Producing Party can readily identify, and the Producing Party shall cooperate and provide such information promptly.

4. Inadvertent Production. The inadvertent production of any material constituting or containing attorney-client privileged information or work-product, or constituting or containing information protected by applicable privacy laws or regulations, shall be governed by provisions contained in Protective Order entered in this action.

B. ELECTRONICALLY STORED INFORMATION

1. Production in Reasonably Usable Form

- a. The parties shall produce electronically stored information in reasonably usable form. Except for documents produced in native format as agreed herein or as agreed hereafter by the parties, such reasonably usable form shall be the single-page TIFF-image format with extracted or OCR text and associated metadata set out in Attachment A (defined as "TIFF-Plus format"), which is incorporated in full in this protocol. Notwithstanding the foregoing, the Receiving Party, for good cause explained in the request, may request native format versions of specifically identified ESI produced originally in TIFF-Plus format. Provided that the requests: (1) are reasonable in volume; (2) specifically identify by bates number the ESI produced originally in TIFF format; and (3) seek files that are not redacted or otherwise cannot be produced in their native form, the Producing Party shall respond in good faith to such requests. For good cause and at its discretion, the Producing Party may produce certain documents in native form with slipsheets in the format set forth in Appendix A, Paragraph A.15.
- b. Redactions. The Producing Party may redact from any TIFF image, metadata field, or native file material that is protected from disclosure by applicable privilege or immunity, that is governed by the European Data Privacy Directive or other applicable privacy law or regulation, that contains sensitive healthcare information, that contains commercially sensitive or proprietary non-responsive information, or

that the Protective Order entered in this Action allows to be redacted. Each redaction shall be indicated clearly on the face of any TIFF image, stating the fact of redaction over the redacted portion of the document with the word “REDACTION” and the word “PRIVILEGE” or “OTHER” as the reason for redaction. In preparing document families for production, the Producing Party also may withhold entire attachments that are wholly non-responsive but must provide slip sheets in their place.

- c. Each Party may make requests, for good cause, for production of specifically identified documents in color.

2. Electronic Spreadsheets, Presentations, Desktop Databases, and Multimedia Files

Electronic spreadsheets (*e.g.*, Excel), electronic presentations (*e.g.*, PowerPoint), desktop databases (*e.g.*, Access), and audio/video multimedia files, SAS data and corresponding program codes if program codes identified by file extension by the Receiving Party that have been identified as responsive shall be produced in native format, unless they are authorized to be redacted in accordance with Paragraph 1.b above. After such redactions, the Producing Party either shall produce the redacted file in the reasonably usable form set out in Attachment A or shall produce the redacted copy in native format.

Additionally, the Producing Party shall not deny reasonable requests for native format production of Microsoft Word files on a document-by-document basis for good cause, which shall be explained in the request.

3. Enterprise Databases and Database Management Systems

For database and database management systems for which data already has been collected in other litigations or for some other purpose as of the date of this Order, the Parties shall accept such data in the form collected, provided that data that is stored in and exportable in a parsable, analyzable format (*e.g.*, CSV or Excel) is produced as such without prejudice to the Receiving Party to later seek production in a different format. For database and database management systems for which data has not already been collected for this litigation as of the date of this Order, the Parties shall meet and confer regarding the appropriate form of production prior to collection of data. In instances in which discoverable electronically stored information in an enterprise database or database management system (*e.g.*, Oracle, SQL server, DB2) can be produced in an already existing and reasonably available report, the Parties shall collect and produce, in the reasonably usable TIFF-image form described in Attachment A, the discoverable material in that report format without prejudice to the Receiving Party to later seek production in a different format.

4. Additional Procedures for Native Format Files

- a. Procedures for assigning production numbers and confidentiality information to files produced in native format are addressed in Appendix A, Paragraph A.15.
- b. Any Party seeking to use, in any proceeding in this Action, files produced in native format shall do so subject to the following:

i. If the native file has been converted to TIFF-image or hardcopy, the original production number and confidentiality designation shall be stamped on each page of the resulting TIFF-image or hardcopy document representing the original native-format file, with a suffix added to the production number to identify the particular page in the file (*e.g.*, XYZ00001_001). In addition, the MD5 or SHA-1 hash value of the native file from which the TIFF-image or hardcopy document was generated shall be placed on the first page of the TIFF-image or hardcopy document.

ii. If the file will be used in its native format, the party seeking to use the native file shall create and attach thereto a slip sheet which provides the production number and MD5 hash value of the file as well as any confidential designation.

iii. Use of a file in native format, or use of a TIFF-image or hardcopy document representing the original native-format file shall constitute a representation that the file being used is an accurate and complete depiction of the original native-format file.

5. Use of Search Filters

- a. To contain costs in the identification of relevant ESI for review and production, the Parties may meet and confer to discuss either the use of reasonable search terms, file types, and date ranges or the use of advanced search and retrieval technologies, including predictive coding or other technology-assisted review. During such discussions, the Producing Party shall retain the sole right and responsibility to manage and control searches of its data files, including the right to make revisions to search-term or advanced-technology procedures in order to make them more accurate and cost-effective. If such revisions are needed, the Producing Party will so notify the Requesting Party and the Parties shall meet and confer regarding the revisions if the Requesting Party does not agree to them.
- b. Janssen will propose a list of search terms to Plaintiff within 15 days of entry of this Order. Plaintiffs will meet and confer with Janssen regarding those terms within 30 days of the entry of this Order. Agreement on search terms will be completed promptly, but such agreement will not itself prevent Plaintiffs from seeking additional search terms throughout the course of discovery as limited by the deadlines set forth in a Discovery Scheduling Order to be agreed upon by the parties, subject to Janssen's agreement or the Court's intervention.
- c. The fact that any electronic file has been identified in agreed-upon searches shall not prevent any Party from withholding such file from production on the grounds that the file is not responsive, that it is protected from disclosure by applicable privilege or immunity, that it is governed by the European Data Privacy Directive or other applicable privacy law or regulation, that it contains commercially sensitive or proprietary non-responsive information, or that the Protective Order entered in this Action allows the file to be withheld.
- d. Nothing in this section shall limit a Party's right reasonably to seek agreement from the other Parties or a court ruling to modify previously agreed-upon search terms,

later requests for search term validation, or procedures for advanced search and retrieval technologies.

- e. If documents that are collected were segregated by product name in the ordinary course of business within departmental files or databases, the Producing Party shall consider whether the application of search terms to this data is appropriate and identify to the Receiving Party upon production which document sources, if any, were not culled by search terms.

6. Email Threading.

- a. Email threads are email communications that contain prior or lesser-included email communications that also may exist separately in the Party's electronic files. A most inclusive email thread is one that contains all of the prior or lesser-included emails, including attachments, for that branch of the email thread. The Parties agree that email thread suppression will not be applied to produced emails. The Producing Party may produce the prior or lesser included email threads separately in a subsequent production that shall be made within thirty (30) days after each production containing the most inclusive email thread. However, where a most inclusive email thread is either redacted or withheld for privilege, the Producing Party need only include the most inclusive email thread on a privilege log and need not produce or log the prior or lesser-included emails within the same thread.

7. Avoidance of Duplicate Production

"Duplicate ESI" means files that are exact duplicates based on the files' MD5 or SHA-1 hash values. The Producing Party need produce only a single copy of responsive Duplicate ESI. A Producing Party shall take reasonable steps to de-duplicate ESI globally (*i.e.*, both within a particular custodian's files and across all custodians). Entire document families may constitute Duplicate ESI. De-duplication shall not break apart families. When the same Duplicate ESI exists in the files of multiple custodians, those persons shall be listed in the Other_ Custodians field identified in Paragraph A.14(c) of Attachment A.

C. DOCUMENTS THAT EXIST ONLY IN HARDCOPY (PAPER) FORM

A Party shall produce documents that exist in the normal course of business only in hardcopy form in scanned electronic format, redacted as necessary, in accordance with the procedures set out in Attachment A. Except as set out in section A.3 above, the scanning of original hardcopy documents does not otherwise require that the scanned images be treated as ESI.

DATED: October 25, 2016

DRINKER BIDDLE & REATH LLP

By: /s/ Michael C. Zogby
Michael C. Zogby
600 Campus Dr.
Florham Park, NJ 07932-1047
Phone: (973) 549-7209
Fax: (973) 360-9831
Michael.Zogby@dbr.com

Attorneys for Defendants Johnson & Johnson and
Janssen Pharmaceuticals, Inc.

DATED: October 25, 2016

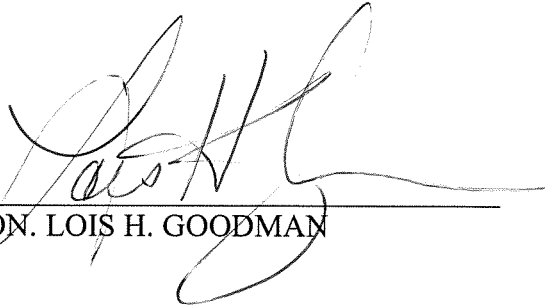
SEEGER WEISS LLP

By: /s/ Christopher A. Seeger
Christopher A. Seeger
550 Broad Street, Suite 920
Newark, NJ 07102
Phone: (973) 639-9100
Fax: (973) 639-9393
Email: cseeger@seegerweiss.com
Plaintiffs' Co-Lead Counsel

IT IS SO ORDERED

DATED: _____

6/7/17



HON. LOIS H. GOODMAN

- A.1. Image Files. Files produced in *.tif format will be single page black and white *.tif images at 300 DPI, Group IV compression. To the extent possible, original orientation will be maintained (*i.e.*, portrait-to-portrait and landscape-to-landscape). Each *.tif image will be assigned a unique name matching the production number of the corresponding page. Such files will be grouped in folders of no more than 1,000 *.tif files each unless necessary to prevent a file from splitting across folders. Files will not be split across folders and separate folders will not be created for each file. Production (“Bates”) numbers shall be endorsed on the lower right corner of all images. This number shall be a unique, consistently formatted identifier that will:
- a) be consistent across the production;
 - b) contain no special characters; and
 - c) be numerically sequential within a given file.

Bates numbers should be a combination of an alpha prefix along with an 8 digit number (e.g. ABC0000001). The number of digits in the numeric portion of the Bates number format should not change in subsequent productions. Confidentiality designations, if any, will be endorsed on the lower left corner of all images and shall not obscure any portion of the original file.

- A.2. File Text. Except where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, full extracted text will be provided in the format of a single *.txt file for each file (*i.e.*, not one *.txt file per *.tif image). Where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, the redacted *.tif image will be OCR'd and file-level OCR text will be provided in lieu of extracted text. Searchable text will be produced as file-level multi-page UTF-8 text files with the text file named to match the beginning production number of the file. The full path of the text file must be provided in the *.dat data load file. The text file shall include interlineated image keys/bates numbers sufficient to show, for all TIFF-image pages, the bates-numbered page of the associated text.

- A.3. Word Processing Files. Word processing files, including without limitation Microsoft Word files (*.doc and *.docx), will be produced in *.tif format as set forth above with tracked changes, comments, and hidden text showing. Microsoft Word documents with track changes shall be produced in color in *.jpg format. Word processing files originally produced in this format may be re-produced in their native format pursuant to the procedure set forth in section B(1)(a).

- A.4. Presentation Files. To the extent that presentation files, including without limitation Microsoft PowerPoint files (*.ppt and *.pptx), are redacted and therefore produced in *.tif image format, such *.tif images will display comments, hidden slides, speakers' notes, and similar data in such files.

- A.5. Spreadsheet or Worksheet Files. To the extent that spreadsheet files, including without limitation Microsoft Excel files (*.xls or *.xlsx), are redacted and therefore produced in *.tif image format, such *.tif images will display hidden rows, columns, and worksheets, if any, in such files. If redactions can be made natively, then the native redacted spreadsheet shall be produced.
- A.6. Parent-Child Relationships. Parent-child relationships (*e.g.*, the associations between emails and their attachments) will be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent email or ESI record. Parent-child relationships will be identified in the data load file pursuant to paragraph A.14 below.
- A. 7. Dynamic Fields. Documents containing dynamic fields such as file names, dates, and times will be produced showing the field type (*e.g.*, “[FILENAME]” or “[AUTODATE]”), rather than the values for such fields existing at the time the file is processed.
- A.8. English Language. To the extent any data exists in more than one language, the data will be produced in English, if available. If no English version of a file is available, the Producing Party shall not have an obligation to produce an English translation of the data.
- A.9. Embedded Objects. Some Microsoft Office and .RTF files may contain embedded objects. Such objects typically are the following file types: Microsoft Excel, Word, PowerPoint, Project, Outlook, and Access; and PDF. Subject to claims of privilege and immunity, as applicable, objects with those identified file types shall be extracted as separate files and shall be produced as attachments to the file in which they were embedded.
- A.10. Compressed Files. Compressed file types (*i.e.*, .CAB, .GZ, .TAR, .Z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.
- A.11. Encrypted Files. The Producing Party will take reasonable steps, prior to production, to unencrypt any discoverable electronically stored information that exists in encrypted format (*e.g.*, because password-protected) and that can be reasonably unencrypted.
- A.12. Scanned Hardcopy Documents
- a) In scanning hardcopy documents, multiple distinct documents should not be merged into a single record, and single documents should not be split into multiple records (*i.e.*, hard copy documents should be logically unitized).

- b) For scanned images of hard copy documents, OCR should be performed on a document level and provided in document-level *.txt files named to match the production number of the first page of the document to which the OCR text corresponds. OCR text should not be delivered in the data load file or any other delimited text file.
- c) In the case of an organized compilation of separate hardcopy documents—for example, a binder containing several separate documents behind numbered tabs—the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the family fields set out below.

A.13. Production Numbering.

In following the requirements of Paragraph A.1, the Producing Party shall take reasonable steps to ensure that attachments to documents or electronic files are assigned production numbers that directly follow the production numbers on the documents or files to which they were attached. If a production number or set of production numbers is skipped, the skipped number or set of numbers will be noted. In addition, wherever possible, each *.tif image will have its assigned production number electronically “burned” onto the image.

A.14. Data and Image Load Files.

- a) Load Files Required. Unless otherwise agreed, each production will include a data load file in Concordance (*.dat) format and an image load file in Opticon (*.opt) format.
- b) Load File Formats.
 - i. Load file names should contain the volume name of the production media. Additional descriptive information may be provided after the volume name. For example, both ABC001.dat or ABC001_metadata.dat would be acceptable.
 - ii. Unless other delimiters are specified, any fielded data provided in a load file should use Concordance default delimiters. Semicolon (;) should be used as multi-entry separator.
 - iii. Any delimited text file containing fielded data should contain in the first line a list of the fields provided in the order in which they are organized in the file.
- c) Fields to be Included in Data Load File. For all documents or electronic files produced, the following metadata fields for each document or electronic file, if available at the time of collection and processing and unless such metadata fields are protected from disclosure by attorney-client privilege or work-product

immunity or otherwise prohibited from disclosure by law or regulation, including the European Data Privacy Regulation, will be provided in the data load file pursuant to subparagraph (a), above, except to the extent that a document or electronic file has been produced with redactions. The term “Scanned Docs” refers to documents that are in hard copy form at the time of collection and have been scanned into *.tif images. The term “Email and E-Docs” refers to files that are in electronic form at the time of their collection.

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
PRODBEG [Key Value]	ABC00000001	Yes	Yes	Beginning production number
PRODEND	ABC00000008	Yes	Yes	Ending production number
PRODBEGATT	ABC00000009	Yes	Yes	Beginning production number of parent in a family
PRODENDATT	ABC00001005	Yes	Yes	Ending production number of last page of the last attachment in a family
CUSTODIAN	Smith, John	Yes	Yes	Custodian(s) that possessed the document or electronic file---multiple custodians separated by semicolon
OTHER_CUSTODIANS	Doe, Jane; Jones, James	Yes	Yes	When global de-duplication is used, these are custodians whose file has been de-duplicated
NATIVEFILE	Natives\\00000001.xls	N/A	Yes	Path and file name for native file on production media
FILEDESC	Microsoft Office 2007 Document	N/A	Yes	Description of the type file for the produced record
FOLDER	\My Documents\Document1.doc	N/A	Yes	Original source folder for the record produced.
FILENAME	Document1.doc	N/A	Yes	Name of original electronic file as collected
DOCEXT	DOC	N/A	Yes	File extension for email or e-doc
PAGES	2	Yes	Yes	Number of pages in the produced document or electronic file (not applicable to native file productions).
AUTHOR	John Smith	N/A	Yes	Author information as derived from the properties of the document.
DATECREATED	10/09/2005	N/A	Yes	Date that non-email file was created as extracted from file system metadata
DATELASTMOD	10/09/2005	N/A	Yes	Date that non-email file was modified as extracted from file system metadata
SUBJECT	Changes to Access Database	N/A	Yes	“Subject” field extracted from email message or metadata properties of the document
FROM	John Beech	N/A	Yes	“From” field extracted from email message
TO	Janice Birch	N/A	Yes	“To” field extracted from email message
CC	Frank Maple	N/A	Yes	“Cc” or “carbon copy” field extracted from email message
BCC	John Oakwood	N/A	Yes	“Bcc” or “blind carbon copy” field extracted from email message
DATESENT	10/10/2005	N/A	Yes	Sent date of email message (mm/dd/yyyy)

				format)
TIMESENT	10:33 am	N/A	Yes	Sent time of email message, time zone set to GMT
DATERCVD	10/10/2005	N/A	Yes	Received date of email message (mm/dd/yyyy format)
TIMERCVD	10:33 am	N/A	Yes	Received time of email message, time zone set to GMT
CONFIDENTIALITY	HIGHLY CONFIDENTIAL	Yes	Yes	Text of confidentiality designation, if any
TEXTPATH	Text\\\.txt	Yes	Yes	Path to *.txt file containing extracted or OCR text
PRODVOL	VOL001	Yes	Yes	Name of the Production Volume
REDACTED	Yes/No	Yes	Yes	Identifies whether a document contains redactions
REDACTION REASON	Privilege	Yes	Yes	Identifies the reason for a redaction

- A.15. Files Produced in Native Format. Any electronic file produced in native file format shall be given a file name consisting of a unique Bates number and, as applicable, a confidentiality designation; for example, “ABC00000002 _Confidential.” For each native file produced, the production will include a *.tif image slipsheet indicating the production number of the native file and the confidentiality designation, and stating “File Provided Natively”. To the extent that it is available, the original file text shall be provided in a file-level multi-page UTF-8 text file with a text path provided in the *.dat file; otherwise the text contained on the slipsheet shall be provided in the *.txt file with the text path provided in the *.dat file.
- A.16. Production Media. Unless otherwise agreed, documents and ESI will be produced on optical media (CD/DVD), external hard drive, secure FTP site, or similar electronic format. Such media should have an alphanumeric volume name; if a hard drive contains multiple volumes, each volume should be contained in an appropriately named folder at the root of the drive. Volumes should be numbered consecutively (ABC001, ABC002, etc.). Deliverable media should be labeled with the name of this action, the identity of the Producing Party, and the following information: Volume name, production range(s), and date of delivery.
- A.17. Encryption of Production Media. To maximize the security of information in transit, any media on which documents or electronic files are produced may be encrypted by the Producing Party. In such cases, the Producing Party shall transmit the encryption key or password to the Requesting Party, under separate cover, contemporaneously with sending the encrypted media. The receiving parties in this matter are on notice that certain data produced may originate from custodians in the European Union and the receiving parties therefore agree to follow the strictest security standards in guarding access to said data.