FDA Investigations Operations Manual 2007

Chapter 5 Excerpt Related to Electronic Records Inspection

5.3.8.3 - Filmed or Electronic Records

When attempting to obtain records, you may find they are stored on microfilm, microfiche, or some form of a computerized management information system as electronic records.

5.3.8.3.1 - Microfilm/Microfiche and Electronic Information

You may encounter records stored on microfilm/microfiche or as electronic records on a computer system. Hard copy records obtained during the course of the inspection from these sources are handled the same as any hard copied records following procedures outline in IOM 5.3.8, 5.3.7.1 and 5.3.8.2.

NOTE: See CPG Section 130.400 for Agency Policy concerning microfilm and/or microfiche records. 21 CFR Part 11 contains information concerning Electronic Records and Electronic Signatures and may be of value to you.

5.3.8.3.2 - Electronic Information Received on CD-R, or other Electronic Storage Media

You may obtain electronic information, databases, or summary data from a firm's databases during an establishment inspection. The methods used must maintain the integrity of the electronic data and prevent unauthorized changes. Do not personally access a firm's electronic records, databases, or source/raw data during the course of an inspection.

When it is necessary to access a firm's data during an inspection:

1. Oversee the firm's personnel accessing their system and have them answer your questions.
2. Request the firm run queries specific to the information of interest.
3. Have the firm generate reports/data to be copied to a CD or other electronic storage media, which you can subsequently analyze, or have the data printed in hardcopy.

Electronic data, such as blood bank databases, drug production records, medical device complaints, service records, returned products and other records are often dynamic data files with real time updating. Information from these files is generally provided at the time of the inspection. Your request may require the firm to develop one or more custom queries to provide the requested information. You must assume the query logic is not validated and take appropriate action to ensure the data is accurate and no data has been accidentally omitted due to a programming logic error occurring at the firm.

When appropriate, a copy of electronic data can be obtained on one or more CD-R, or other electronic storage media. If you provide the diskettes to the firm, use only new, previously unused and preformatted

diskettes. An additional safeguard is to request the firm reformat the disk on their own computer to assure it is usable and "clean".

Any request for electronic information on a CD-R, or other electronic storage media must be made with a computer application in mind and the data obtained must be useful. Request for electronic information should be in a format compatible with software applications knowledgeable to you and available from the Agency. Converting files into different file formats is difficult and should not be attempted without the necessary knowledge and availability of conversion type programs where applicable. If help is needed for file conversion, assistance may be available within the district, region or from DFI HFC-130.

Any CD-R or other electronic storage media containing electronic information received during the course of an inspection should be considered and handled as master copies. The firm may or may not retain a copy of the information provided during the course of an inspection. Ask the individual providing the copy(s) to provide actual CD-R or other electronic storage media labeling information, such as filename(s), date and other information to facilitate their later identification of the CD-R or other electronic storage media and the data provided on the CD-R or other electronic storage media. The name of the appropriate software and version used to ensure readability of the information should also be maintained with the copy of the electronic information.

You should perform a virus scan of the master CD-R or other electronic storage media according to Agency requirements. Each master diskette should be write-protected, labeled and identified as you would any hard copy document.

There are no guarantees the files provided on CD-R or other electronic storage media will be useable data. It is your responsibility to make a working copy of each master CD-R or other electronic storage media. Before making any working copies from the master CD-R or other electronic storage media, confirmation should be made that the write-protection has been activated on each master diskette. You will need to use a computer to view the copied files and verify each file contains the information requested and the information is useable to you. Some electronic data files may be too large to open from a CD-R or other electronic storage media and must be loaded on a hard disk before opening. If this is the case, the file should be put on a subdirectory before opening and viewing.

As a general practice, any findings developed from electronic information provided by the firm should be requested in a hard copy format. The hard copy provided by the firm should then be used as an exhibit to support the investigator's observation. This will preclude or limit any errors that may have occurred from the investigator querying of the electronic information.

The master CD-R, diskettes or other electronic storage media, should be secured to assure the integrity of the data when used in a subsequent enforcement action. Identify the master copy as an exhibit, write-protect diskettes, and place in a suitable container, e.g., FDA-525, and officially seal. Mark the FDA-525 or other container as containing diskettes and to "Protect from magnetic fields." The diskette(s) should be stored as part of the exhibits with the original EIR. See IOM 5.10.5.1.

5.3.8.4 - Requesting and Working with Computerized Complaint and Failure Data

The auditing of FDA regulated firms has found that an increasing number of firms are developing and maintaining computerized complaint and failure data to meet GMP record requirements. Records, hardcopy and electronic, are becoming increasingly voluminous. The auditing of information contained in computerized databases is generally most effectively accomplished with the use of a computer.

Computer auditing of computerized complaints and failure data may require the transfer of electronic data to CD-R or other electronic storage media for you to use in your computer. You should use a computer and application software familiar to you to query information obtained in electronic format. You should not use

the audited firm's equipment or personnel to perform repetitive queries or manipulation of the audited firm's own computerized data.

5.3.8.4.1 - Computerized Complaint and Failure Data

Requesting and obtaining electronic data on CD-R or other electronic storage media is becoming more common during the course of routine inspections. Providing computerized data on electronic media is advantageous to both you and the firm and can result in shorter inspection time. These types of databases contain large numbers of records, which can be easily and quickly queried if they are in electronic format. Inspection time would be lengthened if all such information was only provided in hardcopy format. It may result in you reentering all of the hardcopy data into a new database or reviewing volumes of documents. Be aware if the firm should generate custom software to provide requested electronic records, it would be difficult for you to validate or verify the firm's algorithm used to extract the requested data and ensure that records were not accidentally or deliberately omitted due to programming logic errors, data entry errors, etc.

5.3.8.4.2 - Requesting Computerized Data

Before requesting a copy of computerized data, you should determine several things including information about the size and contents of the database, the program used by the firm, and the program you will use, among others. The following steps are useful in preparing for an electronic record request.

1. Determine the firm's application program used to maintain the data of interest. This may be in a DOS compatible application program such as Access, Excel, Dbase, Paradox, Lotus 123 or others. It is best to obtain data files in a format compatible with application programs you will be using. Large data files with record counts in excess of 10,000 records are best converted to file formats that can be used by programs designed to handle such large databases. There are spreadsheet record limits in some commercial programs that would not allow these application programs to handle much over 5,000 records. Check the program you plan to use to ensure it can handle the file size you will be using.
2. Most large and real-time data files reside in mainframe or network systems requiring programming and downloading to a PC using an [Structured Query Language (SQL)] SQL format. Although data may be captured and downloaded in an SQL format, not all spreadsheet or database application software can load an SQL file. In addition, it may be difficult or impossible to manipulate data in that format. Problems can also be encountered downloading data from Apple computers to an IBM format. Successful conversions are possible if the firm selects the proper conversion format or you have conversion software designed to convert from an Apple to an IBM platform.
3. You may need to request an ASCII (American Standard Code for Information Interchange) text/flat file format. ASCII format is an industry standard, which assigns a unique code to every printable, keyboard, and screen character. An ASCII file should be stripped of all non [-] standard codes that are used by specific application programs for fonts, underlining, tabs, etc. The ASCII text file can be imported by all application programs, and once imported, can be restructured for the specific application program. ASCII delimited is the format of choice, with ASCII fixed length as an alternative. Care must be exercised in

specifying a hard carriage return at the end of each line to be DOS compatible, or additional conversion may be necessary before the file is useable.

4. You should determine what fields of information are routinely captured by the firm. This can be accomplished by requesting a printout of the data structure of the data file or observing the inputting of data at a computer terminal or workstation. It is common for databases to contain numbers or other coded information requiring translations from look up tables to give meaningful text. You should determine if information fields contain coded data, and if so, a code breakdown should be obtained. Information about code breakdowns should be located in the SOPs for that computerized system. Also be aware in relational databases, there may be linking data fields that exist in other tables that should also be considered in the overall data request.
5. If the files are too large to fit on a disk, file compression must be used. If possible, ask that the firm prepare the data in a compression format that is self-extracting. Self-extracting files are executable files and should be virus scanned before and after executing. All CD-R, diskettes or other electronic storage media should be scanned prior to being used on any FDA computer. Whatever compression utility is used, make sure you have the software to manipulate the files as needed.
6. You should always get the total record count of the data file provided by the firm. This count should be verified any time the file is loaded, converted, manipulated, or queried.

5.3.8.4.3 - Identification and Security of CD-R, Diskettes or Other Electronic Storage Media

You should follow these steps to ensure proper identification and security of CD-R or other electronic storage media:

1. Label each CD-R or other electronic storage media
    1. Firm name
    2. Date and your initials
    3. Initials by a representative of the firm (optional) If you provide the diskettes to be used, use only new and preformatted diskettes from an unopened box.
    4. The name of the appropriate software and version to ensure readability of the information
2. Make a working copy of CD-R or other electronic storage media
    1. Write protect the original diskette
    2. Virus scan the original diskette
    3. Copy the original CD-R or other electronic storage media

The original CD-R or other electronic storage media should not be used for manipulating data so as to maintain the integrity of the CD-R or other electronic storage media and data. NOTE: If a virus is detected, do not remove the virus from the source diskette provided by the firm. This may become evidence if it is suspected that the firm intentionally transferred the virus. Attempt to obtain another, uninfected copy of the data file from the firm.

Create a subdirectory on the computer hard drive:

1. Transfer data from the virus-free, working copy of the CD-R or other electronic storage media to your hard drive.
2. Virus scan any decompressed files before and after decompression. (Some virus scan software will scan compressed files but it is safer to scan all foreign files
3. You have now transferred confidential information to the hard drive and that information must be protected.
4. Upon completion of the use of the data, the file must be deleted and totally overwritten with a utility to wipe the data from the hard drive. A delete file operation is not adequate to totally remove the data from the hard drive.
5. Do not leave confidential files in any shared directories or e-mail.

5.3.8.4.4 - Data Integrity of Records Provided by Firm

Many manufacturers are using computers to store records concerning complaints, failure data, returned goods, servicing, testing results and others. Record traceability and data integrity are always concerns when you copy or use computerized data.

1. It is difficult to determine what records are to be designated as originals or copies of original records. It is important, when obtaining hardcopy or copy of computerized data, for you to capture some method of dating. The date of an electronic file can be captured by recording the date and time from a file listing in DOS or with File Manager in Windows. This may not always be possible, but some attempt should be made to date and time stamp electronic data.
2. Requests for most information from manufacturers will require the use of some custom software routine to generate the Investigator's requested information. Any data generated at the request of an Investigator should always be considered custom data. The firm will seldom validate or verify software routines used to generate data in response to your request. You should request a copy of any software program or scripts used to generate the computerized data provided. The request for the software program is not a request for a copy of the application program but a request for the special commands or programs created within the application program for the querying and extraction of data into a new data file. You should review the command structure to ensure it includes all data related to your request.

5.3.8.4.5 - Electronic Information for Official Documentation

During your use of queried data, if you find a violative situation, you should request the firm prepare a hardcopy report of the specific data that depicts the situation. (Do not request an entire copy of the data base and do not rely on the digital database or your extractions from the data to serve as official documentation.) Any records of interest, such as complaints, failure information, etc., noted from querying the computerized data should be copied from original hardcopy documents to support the findings in the database. You should also maintain the procedures or commands you used to find the violative situations in the data base. Follow procedures in IOM 5.3.8.3 for maintaining and identifying original disks.

5.3.8.5 - Listing of Records

If management requests a list of the copies of records you obtain, prepare it in duplicate and leave the original with the firm. Many firms prepare duplicate copies of documents requested during our inspections. In the interests of conserving inspectional time, you may ask the firm to prepare the list of copies concurrently with the photocopying and you then verify the accuracy. Do not use form FDA-484, Receipt for Samples. Describe the circumstances in your report including the name and title of the individual to whom you gave the list. Submit the duplicate list with your report as an Exhibit.

5.3.8.6 - Patient and/or Consumer Identification on Records

During the course of many types of inspections and investigations you will review and collect records which specifically identify (by name) patients or consumers. Under most state Privacy Laws this information is confidential. Some firms we inspect may mistakenly believe this information is not releasable to the federal government. However, Federal laws preempt State laws; with few exceptions we are entitled to review and copy the complete record, including the identifying patient/consumer names. The Agency is then required to maintain the confidentiality of the records/files, as with any confidential record you collect. Any disclosure of the information contained in the record(s) can only be by Law, i.e., judge's order, disclosure, Congressional order, etc.

General, routine guidance is as follows:

1. For records copied as a result of injury or complaint investigation, where you obtain patient identification, the identification should remain intact and stored in the official FDA files. Frequently, medical releases must be obtained from a complainant, consumer or "next-of-kin". At least one or two extra should be obtained and stored in the files.
2. For methadone inspections, continue the Agency policy of deleting patient identification specific to the patient (name, SSN, Driver License #, etc.).
3. For any inspection/investigation involving a regulation required Informed Consent, such as clinical investigations, IRBs, bioequivalence testing, etc., patient identification should remain intact and stored in the official FDA files.
4. For most others, such as MQSA, plasmapheresis, blood donations, etc., only the patient initials and unique identifier supplied by the firm (such as donor number, donation number, etc.) need be routinely retained in the FDA files.

It is not uncommon for a firm to voluntarily purge the documents of the pertinent identifiers as they are copied. You must verify (by direct comparison to the original document) you received an accurate reproduction of the original, minus the agreed to purging, prior to accepting the copy.

As with any inspection there are times when the specific identifiers must be obtained, copied and retained, such as if/when further interview of the patient/consumer could be necessary. If in doubt, obtain the data. It is always easier to delete later than to return to obtain the information, especially in the few cases where questionable practices may result in the loss of the information.

All documents obtained containing confidential identifiers will be maintained as all documents obtained by FDA containing confidential information, i.e., in the official FDA files. Confidential identifiers may be flagged in the official FDA files for reference by reviewers to assure no confidential data are released under FOIA