INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

DISCOVERY BEYOND DOCUMENTS

C. MATTHEW CURTIN, CISSP

MARCH 11-13, 2009

Electronic Information in Wrongful Death Litigation

While the case is not hypothetical, identifying details of the parties and software vendor have been removed. Some examples are simplified to promote focus on our topic.

The story begins with a woman in her mid-thirties with end-stage renal disease secondary to diabetes. Observations and equipment readings from her dialysis sessions were made. Her July 26, 2002 dialysis session ran from 17:15 until 21:21.

```
TIME   COMMENT
00:05  Right chest area sore and both legs hurt.
00:06  Infected.
17:15  Dialysis initiated without difficulty
17:15  lines reversed
17:15  Sodium Linear program initiated
17:15  pt instructed to keep access site expos dur ax
17:35  access site exposed lines intact
17:50  access site exposed lines intact
19:20  access site exposed lines intact
20:57  vanc 1gm iv given for infection
23:33  FORMATTED NOTE, SEE SUMMARY BELOW
23:33  Pt presenting with pain and bloody drainage.
```

Figure 1: Electronic Record Dubbed July 26, 2002 Hemodialysis Session Observations

The patient is admitted to the hospital just over a day later.

```
Infection GRAM - COCCI identified
Infection STAPH AUREUS identified
```

Figure 2: July 28, 2002 Hospital Record

Six days later, the record ends.

```
            08/02/02  HOSP MMC CCU Bed 1
          Discharge:    DX : DEATH - UNKNOWN CAUSE
```

Figure 3: End of Hospital Stay Record

The decedent's family sued, alleging that the dialysis clinic was responsible for the patient's death.

During the course of litigation, various copies of the medical record were produced. Pieces came from different systems. Counsel for the plaintiff had difficulty putting together a complete record. Counsel for the defense had difficulty explaining apparent gaps and contradictions in the records produced.

More than six years into litigation, the defendant produced records again along with a cover letter that read in part:

> Please be advised that some of the records may be in a format different than previously produced. This is due to the change and update in the program used to print the records. However, we believe you should already have copies of these documents from earlier printings.

The plaintiff wanted to make sense of the electronic record with the help of a computer expert. In response to the plaintiff's motion, the court ordered the defendant to pay for the plaintiff's computer expert and the plaintiff's counsel to work with the computer expert in the assessment of the electronic medical record.

Less than forty-five days after the plaintiff engaged a computer expert, a settlement was reached.

How can a case like this offer guidance for successfully managing litigation involving clinical information? Before we address this question, we should examine information in clinical systems.

Data-Driven Applications

We can demonstrate how the electronic medical record in this case worked—and illustrate how similar systems in your own environments very likely work—with a simplified walk through the system. The patient's record was not a continuous stream of data, like what might be found in a handwritten journal where each new entry is added right below the last. Nor was the record like a Microsoft *Word* file or *Excel* spreadsheet, electronic data, but largely visible to the user from beginning to end.

Many software packages used to manage clinical activity are *data-driven applications*, which is to say that the software's behavior is driven by the data in the system. What this means in discovery—and this discovery in particular—becomes clearer as we walk through an example.

Data that make up the patient's record are ultimately stored in a *database*, a software package used to store and to manage potentially large sets of data. A single database is used to store information from one or more of the clinics under the organization’s management. A single computer used for back-end processing and storage, known as a *server*, will support one or more databases.

Software used directly by staff in the clinic is called an *application*. The application will use the database to look up relevant records and then interpret what it finds to display for the user. Input from the user is interpreted by the application and written back to the database. In addition, input to the database can come from clinical equipment, such as a dialysis machine.

All of these parts work together. When a nurse, for example, requests to see a patient’s record, the application will query the database and format the information on-screen, perhaps finding something like Figure 4. If asked to produce an electronic medical record, staff might go to a screen like this for the patient in question and print the screen.

```
SSN: 123-45-6789
Polly Patient           Age:  52      Sex: F
123 Sesame St        Height:  5’5"   Hair: Red
New York, NY 10010   Weight:  131    Eyes: Blue

2009-01-07 7:09 a.m.  Fluid sample.
2009-01-07 7:09 a.m.      Details here.
2009-01-07 7:09 a.m.      More details.
2009-01-07 7:23 a.m.  Noticed bleeding.
2009-01-07 7:23 a.m.      Administered bandage.
2009-01-07 7:27 a.m.  Procedure started.
2009-01-07 7:30 a.m.      Line of clinical system data.
2009-01-07 7:33 a.m.      Line of clinical system data.
2009-01-07 7:36 a.m.      Line of clinical system data.
```

Figure 4: An Example of a View of a Medical Record

In software systems like this, a screen that displays the record is actually aggregating data from many different sources. Systems of this type are typically built atop *Relational Database Management Systems* (RDBMS). These databases store data according to a *schema*, which is a bit like a map to data in the system.

In an RDBMS, data are stored in *tables*, a logical collection of data that are often used together. Those tables are made up of *fields*, typically shown as columns that store the particular attributes of individual items stored in *rows*. Tables that would support our example is shown in Tables 1 and 2.

A separate table might describe information needed for billing, as is shown in Table 3. By using the *ID* consistently, it becomes

ID	*DOB*	*Sex*
14	1963-11-02	M
15	1988-08-14	M
16	1956-03-22	F

Table 1: Table With Patient Sex and Date of Birth

ID	*Height*	*Weight*	*Hair*	*Eyes*
14	68	163	Blonde	Blue
15	72	197	Brown	Green
16	65	131	Red	Blue

Table 2: Table With Patient Description

ID	*SSN*	*NPI*
14	987-65-4321	574658192
15	999-27-3645	472857681
16	123-45-6789	889912341

Table 3: Table With Patient Billing Information

possible for the system to aggregate the data across tables. Other tables would be used to connect information needed to submit billings to the payer.

We now begin to comprehend some of the issues that arise when dealing with electronic discovery. We can see that the construction of the record for display is aggregated from different tables. Also note that the screen shows height not in a combination of feet and inches, but as an integer, a number of inches. This is an example of how the application can perform conversions based on the data to produce a more meaningful display. A similar example can be found in the display of the patient's age, when in fact the data stored show date of birth: age is calculated so as to be up to date at the moment it is displayed.

Next, we turn our attention to the lines toward the bottom the screen used by staff to review the patient's record. Here we are able to identify a critical row in the table showing bedside notes. We can see from the ID and time of the entry where that appears in the "screen view" of the record, and we can see that the description matches. There are also numeric codes in fields labeled "Meds" and "Sig," which we can infer describe medications and a signature.

ID	*DateTime*	*Desc*	*Meds*	*Sig*
23	January 7, 2009 7:22 a.m.	Jargon goes here	241	48
16	January 7, 2009 7:23 a.m.	Noticed bleeding	11	12
89	January 7, 2009 7:23 a.m.	More jargon here	18	

Table 4: Notes from the bed side

With this understanding of how electronic medical records can be constructed, we can move forward to an important legal issue for the litigation.

Why Don't They Match?

Looking in detail at the difference between the early and later productions of records showed an important apparent discrepancy. In the later production, a note appeared showing that a doctor had been called for orders at a critical moment and a new signature appeared in the record. Counsel for the plaintiff could not simply name a new target for deposition to address the issue: the person named in the record had died before the second production.

Two questions then emerged:

1. Why were the productions different? and
2. When was the physician's signature added?

Investigating Data

The most straightforward way to resolve these questions was to look at the data directly, under the application. During the course of my Court-ordered discussions with the defendant's IT staff, I discovered several important facts:

1. The defendant's IT staff did not really know exactly how the application worked;
2. The defendant is not given direct access to the data by the vendor;
3. The defendant had asked the vendor for details about how the data were stored and were rebuffed;
4. The defendant had upgraded their servers during the course of litigation, retiring some servers and re-deploying others for other purposes;
5. The defendant upgraded the software during the course of the litigation and with the help of the vendor "converted" the database from the old data format to a new one; and
6. System backups went back only about one month. The original data used as foundation for the first production were gone.

With this knowledge, I proposed an approach for analysis to retaining counsel. Using raw data going back as far as we could, we would then perform analysis on the database and application to determine if there is additional information that can help us to answer the questions concerning the signature on the medical record. In particular, I was interested in knowing whether the application maintained logs of activity and whether the database maintained activity logs.

The Court ordered the defendant to open its doors to us and to allow us to conduct discovery on the computer systems supporting the critical electronic medical record.

Smoke and Mirrors

After arriving on-site, we were advised that the defendant's corporate counsel would not permit us raw access to any data. We would be permitted only to see a projected version of the application's screen views for the patient's record. The objection was one that I expected: "Release of the raw data would violate HIPAA."

Making the objection especially frustrating was that we were told we would be looking at data that came from a recently-found backup tape that was three years old: in the critical period of time before the upgrades and data conversions.

Because one area of my expertise is information assurance, including security, privacy, and governance, I know the HIPAA Security Rule well. I pointed out that the defendant did have a Business Associate Agreement and that if they would produce it, I would sign it. As an officer of my firm, I also had the authority to bind my firm to an agreement to hold the data confidential. Our standard procedures include the use of cryptography and physical security to protect against accidental disclosure.

We were then told that since we were not "business associates" in any real sense, that would not work. I therefore pointed out that the HIPAA Security Rule, in the same provision that deals with Business Associate Agreements, allows for "other arrangements," and that a Protective Order from the court should address those concerns. In the Order, we would specify particular mechanisms to protect the data, as well as to produce any of our results first to defense counsel to allow for assertion of privilege and irrelevance, to address any concerns that we might be working with the plaintiff's counsel to "mine" the database for new plaintiffs. I also offered to provide language for such an Order.

Defense counsel said that proposed language for a Protective Order might be helpful, but for the time being we would be permitted to see data only as allowed by corporate counsel. We agreed to proceed after I emphasized that if the parties could come to any agreement that would allow us access to raw data, they should do so, as we would be able to render important, relevant, and independent opinions.

Rather than the two days on-site that we planned, we were finished in roughly three hours. IT staff would extract some of the critical data from the database—using a method that they had discovered without the vendor's help. It was not the exact data that we needed, but it was something that would help us to familiarize ourselves with the structure of underlying data.

Conclusion of Litigation

Shortly after the on-site discovery, I made arrangements to travel to the Court for a hearing on discovery. The Court had earlier expressed displeasure with the defendants over discovery. I executed an Affidavit describing what I wanted and what happened in the course of attempting to answer the questions put before me. I was then prepared to take the stand in the hearing, to be cross-examined, and possibly to answer questions directly from the Court, as often happens when I appear.

A day before I was to begin travel, I was advised that a settlement had been reached.

Lessons Learned

Information technology has long been relegated to the basement in many organizations. This separation has been just fine by many in IT; few go into the field because they're easy around other people or want to work with them. In the past few years in particular, however, that separation has become a serious area of risk for organizations of all types, and now even boards of directors are starting to pay attention to how those computer systems work.

For an organization of any size, litigation is a part of business. Discovery is a part of business. Avoidance is not a strategy for success.

IT organizations build systems and services around the needs of business as these are articulated to them. They understand how to attack problems such as reducing cost and increasing productivity. They understand why they need to be able to recover from disasters. Few people in IT, however, have had any exposure to the business processes around management of the litigation portfolio, and few in legal circles have any idea how to ask IT to make their lives easier.

The first step is communication: IT and legal resources need to get to know each other—to get to know a little about what the other does, and how that work is actually performed. This kind of cross-pollination can go a long way toward fostering mutual understanding of the needs and capabilities of each others' work functions.

In IT, systems are often designed and implemented around "use cases," which is to say, how the systems will be used. A similar question exists for litigation: how will the data will be used? Defending the organization in litigation is no less important than issuing invoices and performing other administrative work, so these requirements need to be raised and discussed to ensure that they are addressed.

Working with a computer expert experienced in litigation can help to bridge the gap between IT and the legal departments within an organization. Further, sometimes different systems will have small pieces that can fit together to make a more complete picture. A good expert will also be able to ask questions beyond what a given information system was designed to do, and can look into issues that show what the system *can* do.

Development of a *policy* is also critical. You already understand retention policy issues and have probably attempted to address them with regard to email and documents created on desktop systems. Do you really know how your retention policies are being followed in your clinical systems? Do your IT people? Don't be surprised if the clinicians are in charge of the way that those systems work while the IT people are left in the dark. In my experience, many healthcare organizations operate that way—and don't see why that's a problem until real exposure finally calls.

Policies need to be supported by *procedures*. Those procedures need to spell out not only what to do, but when it should be done in-house and when it should be sent outside. Establishing those relationships before they're actually needed for production is also critical for smooth operation.

Finally, we recommend that corporate clients *train* their responders in their policies and procedures. Going beyond the publication of paperwork is a necessity. We work with clients to test their ability to respond to various types of incidents, including litigation. In these drills, organizations are able to live through a controlled process, to make mistakes that will not prove disastrous in front of a Court, to learn how to improve, and to develop the skill and confidence of staff involved.

Hiding from discovery is a recipe for calamity. Discovery can be handled in an efficient and confident manner only if it is addressed head-on and the organization devotes the necessary time and energy to making sure that it can do the job well.

1. Use training drills to understand:

   (a) How well-prepared organization is for the scenario;

   (b) How well the organization executes its plans;

   (c) How the response compares to other executions of similar scenarios by other organizations; and

   (d) Where the organization can improve its planning and execution.

2. Make drills relevant by assessing litigation portfolio to find:

   (a) High-risk activities: Where likelihood or impact of failure is high;

   (b) High-expense activities: Where expense in litigation portfolio is concentrated; and

   (c) High-frequency activities: Frequent activities.

3. Prioritize followup activity based on findings:

   (a) Establish criteria for prioritization to align portfolio performance with business priorities, e.g.,

   i. Reducing risk,

   ii. Reducing expense,

   iii. Reducing frequency of turning search and production into a "project" or

   iv. Reducing response time.

Figure 5: Method for Addressing Information for Litigation Proactively

C. Matthew Curtin, CISSP is the founder of Interhack Corporation, a computer firm based in Columbus, and Lecturer in the Department of Computer Science and Engineering at The Ohio State University. He has appeared as an expert in federal and state courts, in both civil and criminal proceedings, and on behalf of plaintiffs, defendants, and the court. His work has been used by the U.S. Court of Appeals for the First Circuit to establish standards for the application of Federal wiretap statutes to Web technology in the *Pharmatrak Privacy Litigation*.

Under Curtin's leadership, Interhack's Forensic Computing practice provides services that range from custom software development for analysis to consultation on cost-effective electronic discovery. The firm works with corporate clients and counsel to provide the right balance of risk, utility, and expense in its information management function.