Applying PII fingerprints in security incident analysis

Andrew Padilla
United States., padillaa@us.ibm.com

Martin Oberhofer
United States., martino@de.ibm.com

Ivan Milman
United States., imilman@us.ibm.com

Applying PII fingerprints in security incident analysis

Ivan Milman
IBM
imilman@us.ibm.com

Martin Oberhofer
IBM
martino@de.ibm.com

Andrew Padilla
IBM
padillaa@us.ibm.com

ABSTRACT

Regulations in many countries govern the use of personally identifiable information (PII) in IT systems. A key aspect of these regulations is to retain PII only as long as necessary and delete it immediately afterwards. Organizations should also consider retaining PII only for the minimum period as business requirements demand it for liability reasons. A difficult situation arises for an organization if the possibility of a compromise of PII is detected after the PII has been deleted. Today, in such a situation, the scope of the potential compromise cannot easily be ascertained. Furthermore, the owner of the PII cannot easily be informed. We propose a novel algorithm to generate PII fingerprints which allows the determination of the scope of the affected PII in case a compromise is confirmed. The benefit is the ability to determine the exact scope of a potential compromise.

Keywords

PII fingerprints, sensitive information, regulations, compliance, privacy, healthcare

INTRODUCTION

Personally identifiable information (PII) is information that can reasonably be used to identify a particular individual to whom the information pertains such as an employee, patient, citizen, customer or supplier. A particularly sensitive type of PII is Protected Health Information (defined by HIPAA in the US)[1], which can tie an individual patient to the details of that person's health information. PII is processed in various different types of IT systems today. Examples include Human Resources (HR), master data management (MDM), electronic medical record (EMR) systems, customer relationship management (CRM), enterprise resource planning (ERP) or e-Commerce platform systems. PII is considered to be very sensitive data since it can be associated with a real person. Thus, regulations such as HIPAA (United States), Bundesdatenschutzgesetz (Germany's Federal Data Protection Act), or the Data Protection Act of 1998 (United Kingdom) govern the use of personally identifiable information (PII) in IT systems. A key aspect of these regulations is the mandate to delete PII once the minimal time needed expires. European Union (EU) Directive 95/46/EC on the Protection of Personal Data covers three major areas related to PII. These areas are transparency, legitimate purpose, and proportionality. Proportionality covers consideration of keeping PII only as long as minimally needed. The directive also mandates that PII must be protected from loss, unauthorized disclosure and modification while data is in transit or at rest. Organizations should consider creating a PII retention policy that retains PII only for the minimum period as business requirements demand it which itself is framed within the confines of applicable regulations.

The means to protect sensitive data while at rest, as well as in motion, have been developed over the years. Many different encryption techniques are available for sensitive data at rest. A comprehensive overview can be found in (Schneier, 1996). Similarly, the communication channels for data in motion can be encrypted using techniques like SSL[2] as can the messages themselves. Access to sensitive data can also be restricted using appropriate authentication techniques such as Kerberos (see Chapter 24 in Schneier 1996), time-based authentication or two-factor authentication as well as appropriate data authorization

[1] The regulations mentioned in this section are listed in the references section.

[2] SSL is the abbreviation for secure sockets layer and since version 3.0 known as transport layer security (TLS). RFC 2246 listed in the reference section is for TLS v1.0.

techniques such as LBAC for row and column-based access privileges in the relational database DB2 (see Kenan 2005; LBAC 2011; Natan 2005 and Schneier 2006 for comprehensive discussions on them). All these techniques for sensitive data can be applied to PII as well. However, there is never a 100% guarantee that there will not be a compromise of sensitive data such as PII.

A scenario particularly interesting is the case of detecting the possibility of an unauthorized access after the affected PII data has been deleted as a result of enacted retention policies. In such a scenario, it is difficult to determine the scope of the possible PII compromise. This problem is exacerbated in the case of PHI, which is governed by the HIPAA regulation in the US. Without knowing which PHI might have been affected by a potential unauthorized data access or other potential compromise, it is difficult to comply with the HIPAA regulation breach notification requirements to notify individuals, especially in the case of deleted data where you can no longer easily determine who those individuals are.

We thus introduce in the next section a detailed outline of the scenario as well as why it is interesting. We then propose a novel algorithm which is particularly beneficial in this scenario. We conclude the paper with a short summary of experiences with the algorithm and suggestions for further research.

THE PROBLEM SCENARIO

Figure 1 provides a conceptual overview of the problem scenario. Let's assume there is a persistent PII repository which could be PII data in a relational database hosted on an IT system. There might be various different kinds of traces available such as system logs by the operating system or traces by the database system. We assume that at some point in time as shown in Figure 1 a suspicious security event occurred which could have possibly compromised PII. We further assume that a subset of the PII in the PII repository was later deleted. The final assumption is that due to suspicious system behavior or odd looking entries in traces files the suspicious security event is later detected, but only after this subset of the PII has already been deleted.

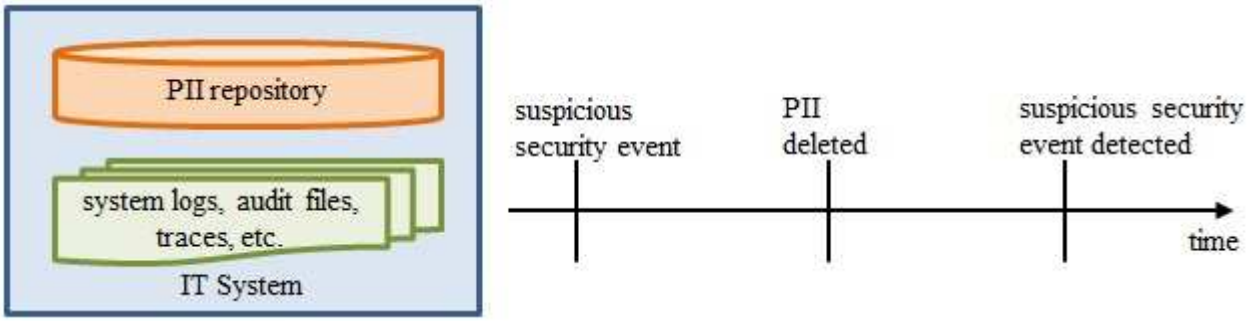

Figure 1: The problem scenario

In this scenario at the time a possible compromise of PII data is suspected an investigation is triggered to determine whether or not an actual breach occurred. During this investigation the following questions will be tough issues:

- How can you determine whose PII was at risk at the time the potential compromise occurred if you have already deleted the PII (after expiry of the permissible retention period to comply with regulations)?
- How can you determine after the PII record has already been deleted which data elements of a PII record were present, and therefore at risk, at the time of the potential compromise? More specifically, was it the whole record or only some fields that were at risk?
- How can you decide where the person to which the PII pertains resides to understand what laws and regulations are applicable and govern in the event of an actual breach?
- How can you inform a person whose PII data might have been compromised, so that they can try to mitigate the impact (such as protecting against identity theft) as early as possible?

None of these issues can be resolved with just applying existing art. For example, if data masking is applied to PII, this technique would convert the PII data into "fake" data. If you must determine whose data got affected by a security incident, you would still need a fingerprint of the real data for analysis as well as access to the real data. Note that the access to the real data is no longer given in our scenario because a subset of the PII has been deleted between occurrence of the potential compromise and detection of the potential compromise. Thus data masking is not useful in this scenario. Similarly, anonymous data sharing techniques based on one-way conversions of data into a non-recoverable form is also not applicable for our scenario. An example for a one-way conversion is a one-way hash functions is MD5 (details in Schneier, 1996). Anonymous

data sharing is useless in our case to determine the scope of a potential PII compromise because it still requires the original data for analysis.

After the introduction of this general scenario, let's take a close look at industry-specific instances of it. For example, in the healthcare industry, patient information is processed in IT systems of healthcare providers such as hospitals and healthcare insurers. Healthcare providers and healthcare insurers often exchange patient information through a Health Information Exchange (HIE) hub which is shown with an example in Figure 2 with a standardized message format such as HL7 (see HL7, 2007). In the US for the healthcare industry, the HIPAA and HITECH regulations govern the use, security and privacy of patient information. Through an HIE, healthcare providers such as a physician and an X-ray lab exchange messages about patients. A physician creates, for example, an order for patient John Smith to receive an X-ray in the physician's electronic medical record (EMR) system. This order gets converted into an HL7 message with a message control number and then forwarded to the HIE. The HIE receives the message and analyzes it to determine the destination which is a certain X-ray lab in our scenario. The HIE also determines and applies any transformation which might be required so that the receiver understands the message. Then the HIE transmits the message to the X-ray lab which then internally creates the order for the X-ray for John Smith. The HIE discards the delivered message and only retains the message control id and the receipt confirmation from the receiver. Note that in this scenario the HIE only transmits the HL7 messages between the participating parties. So if there is an unauthorized access either at the X-ray lab or at the physician's office and the original message was discarded, there would be no way to see whose PII might have been compromised within the HIE.

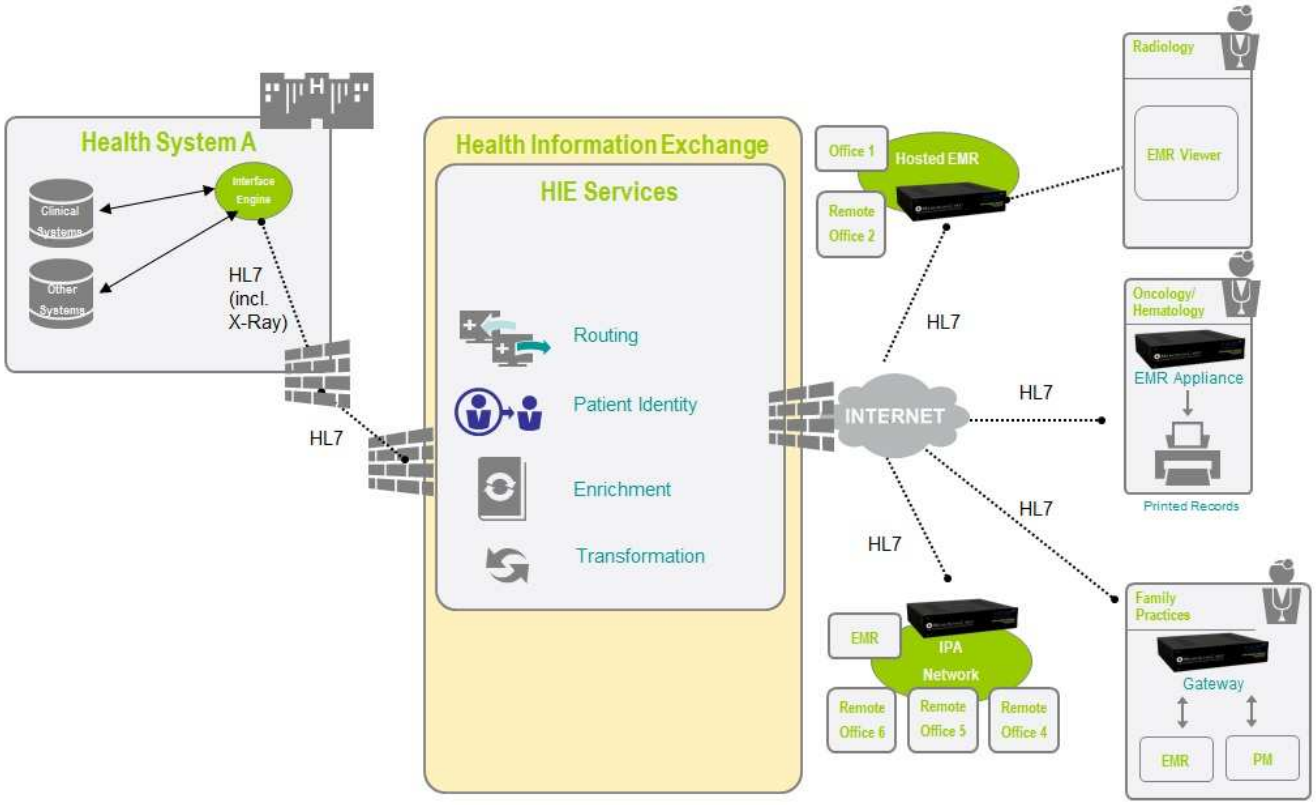

Figure 2: An exemplary HIE architecture

Since PII is also stored in systems which exist cross-industry such as employee information in HR systems or master data in MDM systems variations of the previously outlined scenario are possible for such systems as well.

PII FINGERPRINTING

PII Fingerprinting is a four-step process. First, you need to define the fingerprint record definition. Second, each time PII is created or modified, you need to create appropriate PII fingerprints. Third, these PII fingerprints need to be stored. Fourth, you need to be able to search the PII fingerprints. We describe these steps in more detail in the following sections.

Define A Fingerprint

The first step in creating a PII fingerprint is to create a fingerprint record definition. A fingerprint record is a user defined data construct that indicates the presence or absence of personally identifiable information (PII) for a given (semi-) structured document that contains PII as well as any correlating metadata that does not constitute PII. A creator of a fingerprint definition must first identify candidate PII fields in a document definition that are to form the basis of the fingerprint. For each field identified, a corresponding boolean field in the fingerprint record is created that will indicate whether or not the field was populated in the document. Useful PII candidate fields are any field or fields that alone or in combination may uniquely identify a person. Additional correlating fields which hold actual, subset or derived data values from the source message definition may include dates, locality, opaque identifiers or any other fields that may be useful or otherwise provide a useful context in a subsequent search operation but themselves in part or in whole do not constitute PII. Once a PII fingerprint is defined it can be used to create fingerprints from the source document definition that defined it.

A model structure of a PII fingerprint for an HL7 message is shown in Figure 3:

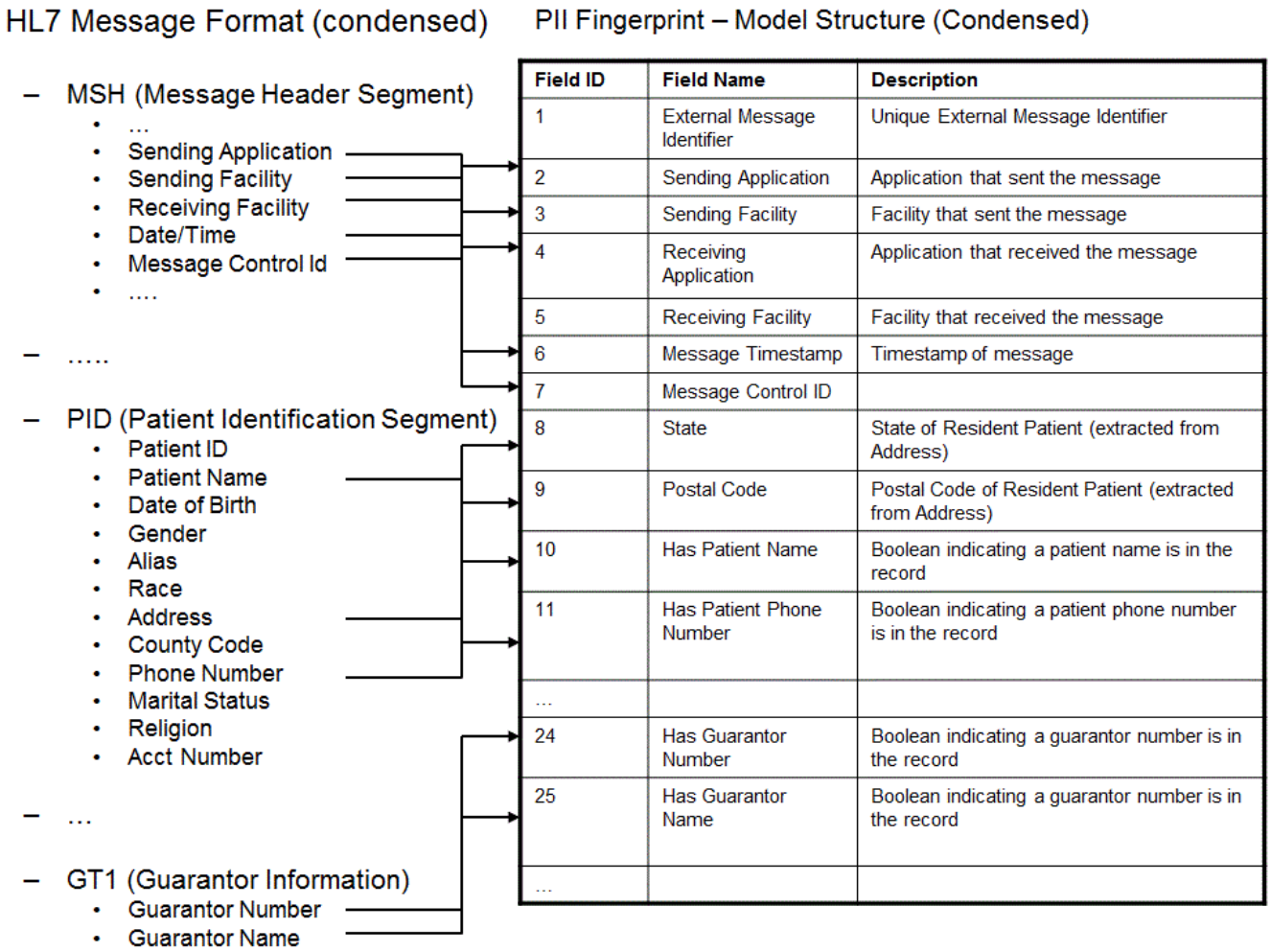

Figure 3: An exemplary HL7 message

Creating and Storing a PII Fingerprint

Once a fingerprint definition is defined, instances of it can be created for archiving. As the document for which the PII fingerprint definition is based is encountered in a system (or systems), a mapping operation between the corresponding fields in the document and their counterpart PII fingerprint fields can be performed which result in the creation of a PII fingerprint record. This record is then submitted to the PII fingerprint system for archival purposes. Optionally, the PII can be also

passed to an escrow service which we discuss in more detail in the implementation section. Figure 4 shows an example of an instance of a PII fingerprint for a specific HL7 message.

HL7 Message (Condensed)

Segment	Element	Field Value
MSH		
MSH	Sending Application	PhysicianEMR
MSH	Sending Facility	MedClinic
MSH	Receiving Application	HospitalEMR
MSH	Receiving Facility	AHospital
MSH	Message Timestamp	9999220152845
MSH	Message Control ID	232423432
...		
PID	Patient ID	1267896
PID	Patient Name	John Doe
PID	Date of Birth	19620218
PID	Gender	MALE
PID	Address	1234 Cabrito Way, Albuquerque, NM, 87101
PID	Phone Number	505-555-1212
....		
24	Guarantor Number	NULL
25	Guarantor Name	NULL
...		

PII Fingerprint for Message (Condensed)

Field ID	Field Name	Field Value
1	External Message Identifier	550e8400-e29b-41d4-a716-446655440000
2	Sending Application	PhysicianEMR
3	Sending Facility	MedClinic
4	Receiving Application	HospitalEMR
5	Receiving Facility	AHospital
6	Message Timestamp	9999220152845
7	Message Control ID	232423432
8	State	NM
9	Postal Code	87101
10	Has Patient Name	TRUE
11	Has Patient Phone Number	TRUE
...		
24	Has Guarantor Number	FALSE
25	Has Guarantor Name	FALSE
...		

Figure 4: An exemplary PII fingerprint

Search For PII Fingerprints

At some point in time, it may be necessary to search the PII fingerprint archive using relevant criteria that will help determine what PII was encountered by participating systems during a given time frame in conjunction with other relevant criteria. Using the PII fingerprint system, a query may be issued with the specified criteria. The PII fingerprint system will return any matches that result from the search performed. This information can then be used as the basis for determining the possible extent of a PII breach.

USE CASE EXAMPLE: HEALTH INFORMATION EXCHANGE

To illustrate how a PII fingerprint system might be used, we will give an example of the interaction between a remote physician office's Electronic Medical Record System (EMR) and a central hospital Lab Information System (LIS). We will assume that these two systems communicate with one another indirectly through the use of an Enterprise Service Bus managed by the hospital. The enterprise service bus is used for routing to/from participating clinical systems as well as for performing transformations to a common message format to enable integration between participating systems. In order to ensure delivery of inbound messages, the Enterprise Service Bus (ESB) persists messages to disk in local queues to ensure delivery in the event an outbound system is unavailable for a period of time or a redelivery of previously a delivered message is required. Local hospital IT staff policy states that all messages delivered by the ESB are archived for a period of two weeks before they are expunged. Secure connectivity between the LIS and EMR system with the ESB is assumed to be provided through some means. The conceptual architecture of this solution environment is shown in Figure 5. As you notice compared to Figure 2 we introduced two new components: The first one is the PII Fingerprinting Services component providing the functionality to define, create and search for PII fingerprints. The second component is the Escrow Services component. This component allows in the case of an incident analysis, assuming the requester's identity has been verified beyond doubt to be legitimate, to recover the encrypted PII fingerprint for more detailed analysis.

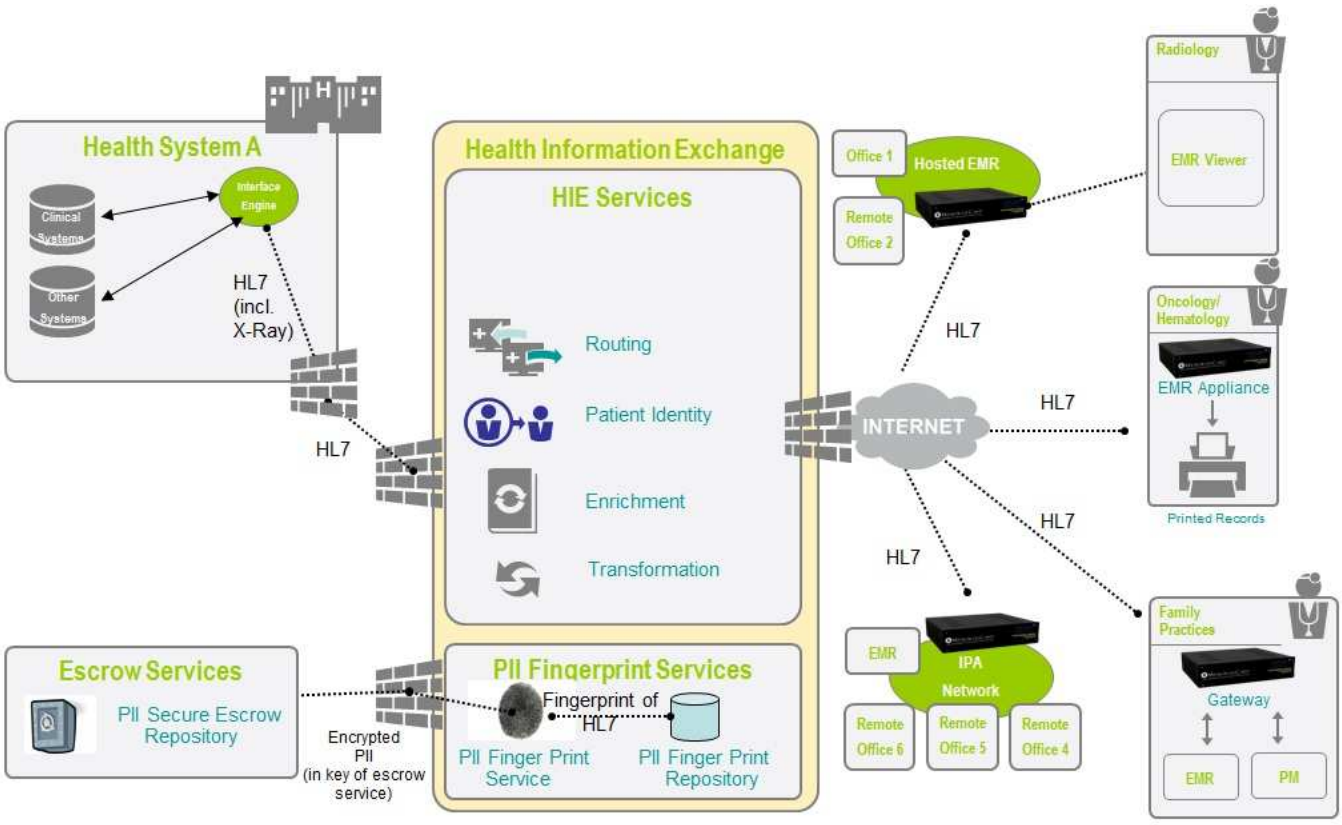

Figure 5: New HIE Solution Architecture

We describe now a step-by-step walkthrough how a PII fingerprint is created by explaining the sequence shown in Figure 6. Numbers in the following text correlate with the appropriate numbers in the sequence diagram.

A patient named John Public takes his yearly visit in the first week of May to his physician (Dr. Roche) for a physical exam (A.1). The physician performs a physical exam (B.1) and then decides to order some blood work (B.2) following the examination. The physician enters the order into his EMR system and also prints out an order requisition form. The form is handed to Mr. Public and an HL7 order message is subsequently transmitted (C.1) from the EMR system to the hospital's ESB system which receives the HL7 message on an Order Message Queue (D.1). Since in our example the optional use of an escrow service is configured the HL7 message is encrypted with the public key of the escrow service (D.2) and then submitted to the escrow service provider (D.3) where it gets stored (H.1).

The hospital's ESB system receives then parses the received message (D.4) and determines that a PII fingerprint must be taken. The fields relevant for the PII fingerprint are determined (D.5) and the PII fingerprint is created (D.6) which is then submitted to the PII fingerprint service (D.7). The PII fingerprint service receives the PII fingerprint (F.1) and stores it in the PII fingerprint store (G.1). The ESB then determines that the order message needs to be routed to the hospital's LIS system (D.8). The HL7 order message is queued for submission to the LIS. The LIS eventually receives the order and generates a record for the order (E.1). John Public arrives at the lab with requisition form in hand to have his blood taken. The technician retrieves his record in the LIS upon receipt of the order requisition form and then draws John Public's blood. The samples are sent to the lab for processing. The blood tests are performed and the results are entered into the LIS system (E.2). These results are subsequently submitted by the LIS (E.3) to the hospital ESB (D.9). For the ESB, just another HL7 message arrived and the configured logic determines that this message also needs a fingerprint to be taken. Thus, the interesting fields for the PII fingerprint are extracted (D.10), a PII fingerprint is created again (D.11) and submitted to the PII fingerprint service again (D.12). The PII fingerprint service receives the fingerprint (F.2) and stores in the PII fingerprint store (G.2) again. Then the ESB routes the HL7 result message back to Dr. Roche's EMR system (D.13) which receives the results (C.2). Dr. Roche reviews the results (B.3) and communicates (B.4) to John Public that his test results are within normal range.

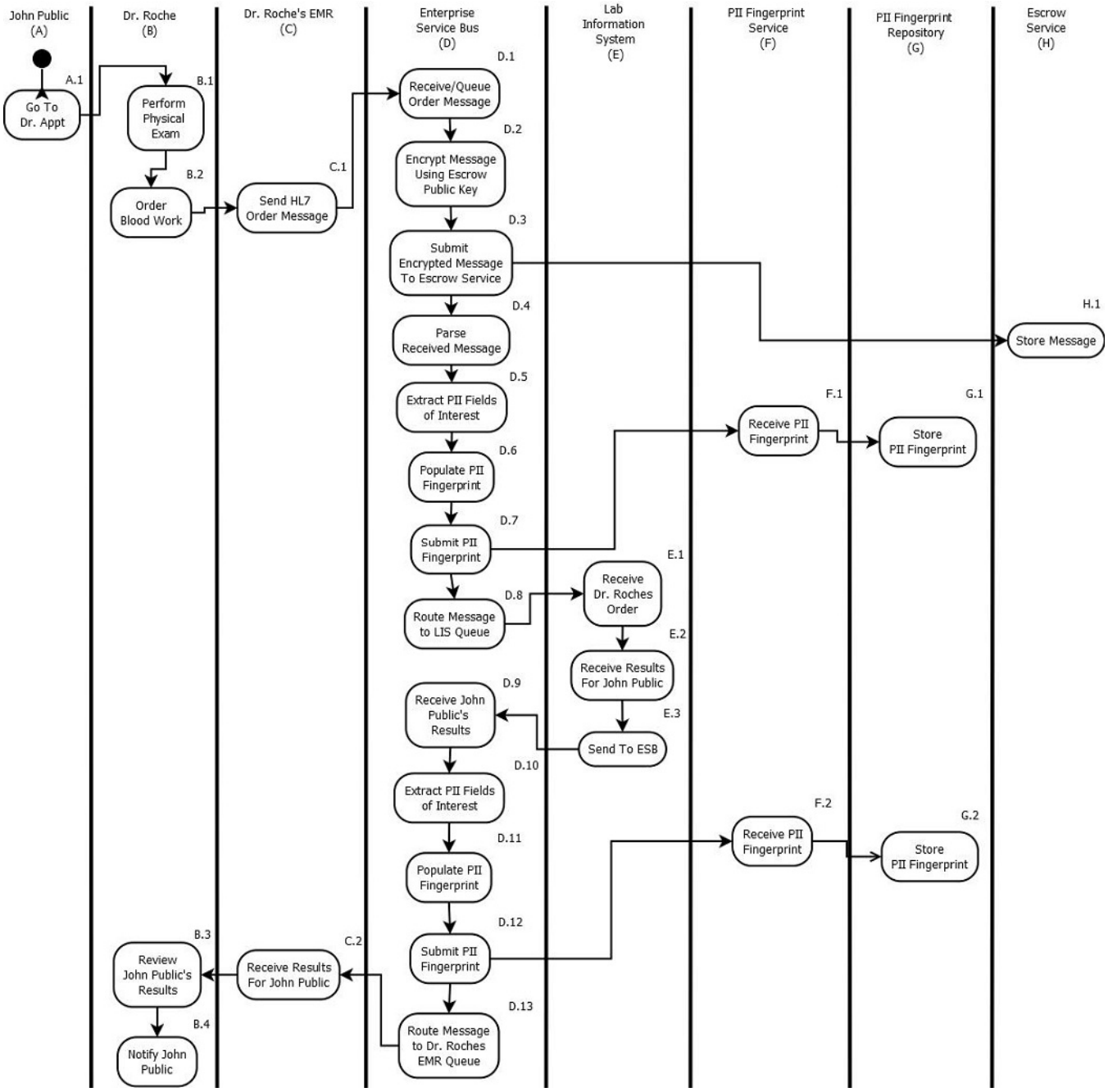

Figure 6: Sequence Diagram showing the creation of an PII fingerprint

We describe now a step-by-step walkthrough how a suspected security incident triggers a search by explaining the sequence shown in Figure 7. Numbers in the following text correlate with the appropriate numbers in the sequence diagram.

A month later, the hospital network IT staff discover that several unauthorized accesses occurred (A.1) on the ESB host system during the month of May. The IT staff needs to perform an audit of what PII was resident on the ESB host system during the timeframe of the intrusion. Fortunately they have integrated a PII fingerprinting solution whereby they can search (A.2) for potential records affected using various constraints available in the PII record definition that was defined by the IT staff. The PII fingerprinting service receives the search queries (B.1) and conducts a search based on the search parameters on the

PII fingerprint store (C.1), determines the results (C.2) which are then processed by the PII fingerprinting service (B.2) and returned to the requester (B.3). Then the hospital IT staff receives the results (A.3) and notifies as needed relevant parties (A.4) to determine what course of action should be taken (if any) to remediate the potential unauthorized access.

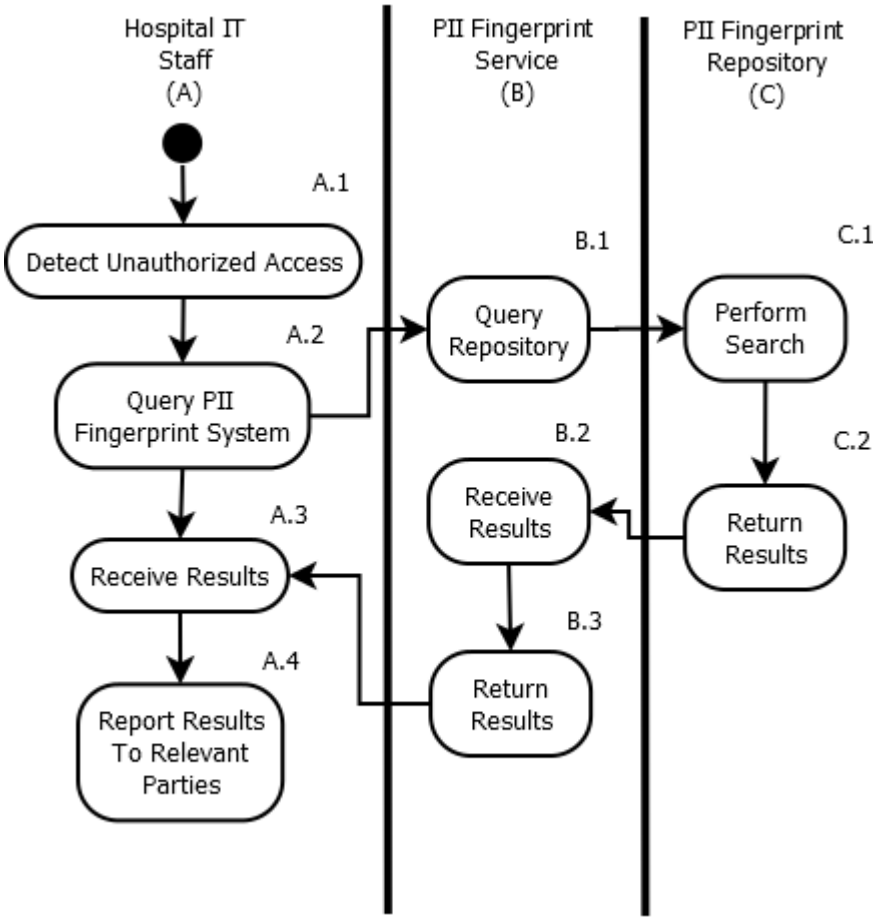

Figure 7: Sequence Diagram showing the detection of an incident and the search process

The sequence diagram shown in Figures 6 and 7 describe the events that were triggered within participating systems with respect to John Public's physical exam and how the PII fingerprinting solution was integrated into the information flow and subsequently used to provide meaningful information on PII that is no longer available.

PRACTICAL RESULTS

The techniques used in this paper for generating PII fingerprints have been applied as an experiment to a derived subset of HL7 messages. The fingerprints were generated after the fact, as opposed to while the HL7 messages were in flight, so operational systems were not impacted. The resulting fingerprints were put into spreadsheets and databases separated from the systems with PII, and used for simple analyses of information at risk, such as

- How much PII is moving thru the system (not all HL7 messages have PII)
- What is the PII to geography mapping (for legal notification thresholds)?
- What is the frequency of the different types of PII (names, SSNs, etc.) in the system?

The fingerprints and analysis were judged to be successful in answering the type of questions above. However, there are two areas that impact any results:

1. Data Quality: Often messages did not include full information about addresses (such as postal codes, states, etc.), so classifying a given message with the relevant locale was challenging. In this initial experiment, we tried to remediate this thru other related information, such as phone number exchanges (for example, +1-

512-658-xxxx is a phone number in Austin, Texas, or information about the location of the facility where treatment was made. This information is not authoritative – one potential enhancement would be to use address information from a third party provider like AddressDoctor to augment the locale analysis.

2. Data Duplication: Many messages contain the same information about the same patient or guarantor. Collapsing this information would potentially be a more accurate way of counting PII. If the information in the message is of consistent quality (or can be consistently standardized), then a common identifier could be used to match fingerprints. The challenge is using a common identifier that is not in and of itself PII (such as a one-way transform of key fields). A variation on this method was attempted with some success in the experiment, but more research should be done here.

CONCLUSION

We introduced a novel PII fingerprinting algorithm in this paper and showed some first practical results. Future improvements are possible in the area of improving data quality in conjunction with the PII fingerprinting algorithm because for example it might be necessary for legal reasons to exactly know which legislation is applicable based on the patients' address information.

REFERENCES

Bundesdatenschutzgesetz (Germany's Federal Data Protection Act), (1990), http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf

Data Protection Act (UK), (1998), http://www.legislation.gov.uk/ukpga/1998/29/contents#pt4-l1g36

European Union (EU) Directive 95/46/EC on the Protection of Personal Data, (1995), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1996), http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html

HL7 Standard 2.5.1, (2007), http://www.hl7.org/implement/standards/product_brief.cfm?product_id=144

Kenan, K.. (2005) *Cryptography in the Database: The Last Line of Defense,* Addison-Wesley Professional.

Label-based access control (LBAC) in IBM DB2 v9.7, (2011), http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.admin.sec.doc%2Fdoc%2Fc0006307.html

Natan, R. B. (2005) *Implementing Database Security And Auditing*, Digital Press.

Schneier, B. (1996) *Applied Cryptography*. 2nd Edition, John Wiley & Sons, New York.

Transport Layer Security protocol v1.0 by IETF, (1999), http://tools.ietf.org/html/rfc2246