Global Information Assurance Certification Paper

Encryption Implementation Specification
Section 164.312(E)(2)(ii)

GIAC HIPAA Security Certificate (GHSC)
Practical Assignment – Version 1.0

Eric Conrad
June 3rd, 2004

Abstract

This document explains the encryption implementation specification (part of the transmission standard), which is described in the technical safeguards section of the HIPAA Security Standards final rule. The environment of GIAC Health is described. Then the encryption implementation specification is explained. An encryption policy is detailed, followed by an audit procedure for verifying compliance. Finally, appendices explain details on capturing transmitted internet EPHI, sample Intrusion Detection rules for alerting unencrypted internet EPHI, and a list of protected health identifiers.

Assignment 1 -- Define the Environment

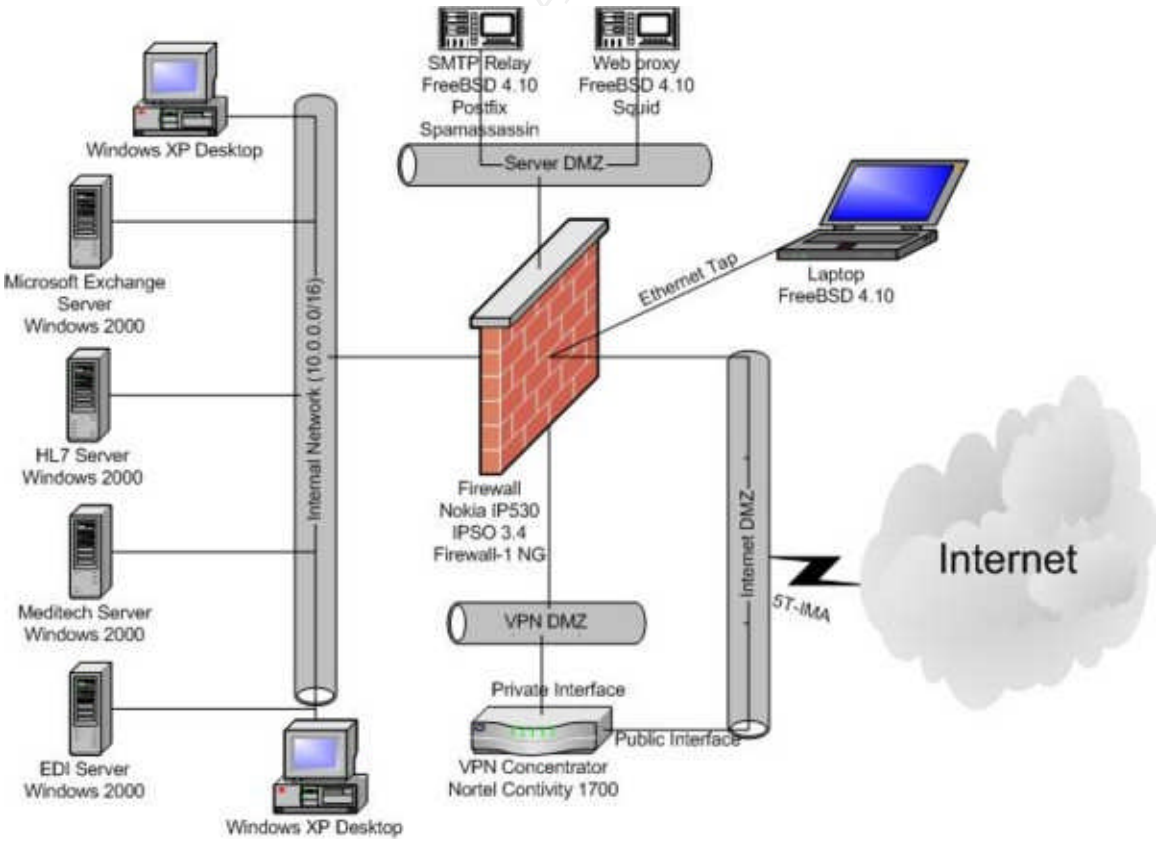
GIAC Health is a large urban hospital. Medical applications run on servers located at the hospital data center. Windows client PCs are located throughout the facility. The primary medical application is Meditech, accessed via Meditech clients running on the client PCs.

The hospital data center has a 5T-IMA (5 bundled T1s) internet connection. The internet firewall has 4 interfaces: internet, VPN DMZ, Server DMZ, and internal. Internal network subnets are in the 10.0.0.0/16 RFC1918 netblock.

A VPN concentrator is used to transmit EPHI (such as lab results, EDI, or HL7 transactions) via encrypted IPSEC tunnels to facilities around the world. Remote users may also connect via client VPN connections.

Additional medical applications such as claims availability via NEHEN (New England Healthcare EDI Network) are accessed via the web.

The security team has a FreeBSD laptop loaded security tools such as tcpdump, ngrep, Snort, etc. Passive ethernet taps are used to 'sniff' network traffic at locations such as the firewall's internet interface.



Assignment 2 -- Explanation

The encryption implementation specification is part of the transmission standard, which is designed to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[1] Section 164.312 (e) (2) (ii) of the HIPAA Security final rule reads:

> Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate[2]

EPHI is the commonly-used acronym for Electronic Protected Health Information, which is "individually identifiable health Information" that is "Transmitted by electronic media" or "Maintained in electronic media."[3]

EPHI can be in 2 states: transmitted (moving) and maintained (stored). EPHI stored on a hard drive is at stored, and EPHI sent via a LAN is transmitted, for example. One twist is a CD containing EPHI which is physically carried is 'transmitted' (moving) via electronic media (the CD), but that transmission is not via an 'electronic communications network', and is not subject to the encryption implementation specification.

Transmitted EPHI should be encrypted "whenever deemed appropriate." When is it appropriate to encrypt transmitted EPHI? The preamble to the final HIPAA security rule sheds more light on this issue:

> …we agree that encryption should not be a mandatory requirement for transmission over dial-up lines... Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.[4]

EPHI should be encrypted when transmitted via an insecure network such as the internet. The next question is what encryption cipher (a.k.a. algorithm) should be used? The encryption implementation specification does not describe a specific cipher or cryptographic key bit length; the preamble states:

> We maintain that it is much more appropriate for this final rule to state a general requirement for encryption protection when necessary and depend on covered entities to specify technical details, such as algorithm types and strength.[5]

Cipher choice and cryptographic key bit length should be based on a covered entity's risk analysis and current best security practices.

The goal of the encryption implementation specification is to ensure that EPHI transmitted over an insecure communications network such as the internet is encrypted via an appropriate cipher.

Assignment 3 -- Policy

This policy is based on the format of the policies found at:
http://www.sans.org/resources/policies/

Policy for Transmitted Electronic Protected Health Information (EPHI)

1.0 Purpose

The purpose of this policy is to protect the confidentiality and integrity of Electronic Protected Health Information (EPHI) which is transmitted via communications networks.

2.0 Scope

The scope of this policy includes all employees or contractors of <Company Name> who are responsible for transmitting EPHI via communications networks.

3.0 Policy

EPHI transmitted via an insecure network such as the internet must be transmitted via an approved method and encrypted via an approved cipher.

Transmission of unencrypted EPHI via an insecure network is forbidden. Any form of encryption that is not explicitly approved is also forbidden.

3.1 Insecure Networks

An insecure network is a network that lacks proper security controls: insecure networks may expose unencrypted EPHI. Examples of insecure networks include (but are not limited to) the internet, unencrypted wireless networks, and poorly-secured private networks.

The <Company Name> wide area network is considered secure. EPHI transmitted exclusively within the WAN is not subject to this policy.

3.2 Approved Methods for Transmitting EPHI

The following methods for transmitting EPHI are approved:

- Connection-based: Point-to-Point VPN
- Remote internet access: VPN client connection
- Web-based: Secure Socket Layer (SSL)
- File-based: Secure Copy (SCP)

All other forms of EPHI transmission (including email) are forbidden.

3.3 Approved EPHI Encryption Ciphers

Approved encryption ciphers (a.k.a. algorithms) and minimum bit lengths, in order of preference are:

AES: 192 bits
Triple DES (3DES): 168 bits
RC4: 128 bits

Use the strongest available cipher. Longer bit lengths may be used; shorter lengths are forbidden.

Any cipher not explicitly allowed is denied.

4.0 Enforcement

All <Company Name> employees and contractors are responsible for adhering to this policy. Violation of this policy may result in disciplinary action, up to and including termination of employment.[6]

5.0 Definitions

AES: Advanced Encryption Standard, an encryption mechanism. Bit lengths include 128, 192, and 256 bits.
DES: Data Encryption Standard, an encryption mechanism. 'Single DES' encryption is 56 bits, 'Triple DES' encryption is 168 bits.
Cipher: an encryption algorithm
EPHI: Electronic Protected Health Information. Personally-identifiable Health Information that is in electronic form (disk, network, etc). Paper copies, paper faxes, and similar 'hard copy' media are not considered 'electronic'.
RC4: an encryption mechanism. Commonly used for 128-bit SSL encryption.
SCP: Secure Copy, a method to copy files via an encrypted connection
VPN: Virtual Private Network, a method for making secure network connections via insecure networks
WAN: Wide Area Network

6.0 Revision History

1.0 Initial version

Assignment 4 – Auditing

Phase 1: Verify firewall and VPN configuration

Step 1: Compose a list of foreign IP addresses which communicate with the EDI, HL7, and Meditech servers.

Inspect these servers for connections to remote networks.

The 'netstat' command will show all network connections:

```
C:\>netstat -an | find "ESTABLISHED"
  TCP  10.0.0.100:4981  192.168.82.68:1142  ESTABLISHED
  TCP  10.0.0.100:4985  10.0.0.110:7851     ESTABLISHED
  TCP  10.0.0.100:6688  172.16.45.67:9999   ESTABLISHED
```

The local subnet is 10.0.0.0/16: the IP addresses highlighted in red are foreign networks. Run this command repeatedly over a period of time to identify as many connections as possible.

Check any application-level configuration on these servers for configured foreign networks or hosts. Each application will be different: ask the application analysts to retrieve this information.

Inspect the firewall logs for all entries with a source address of the EDI, HL7, or Meditech Servers. Note that the internal addresses may be translated to public IP addresses via NAT (Network address Translation).

Step 2: Run 'tracert' from the servers to each identified foreign IP address or network to identify the network path.

```
C:\>tracert 192.168.82.68
```

Note the egress path.

Step 3: Inspect the egress path for each foreign IP address, and note whether the path traverses the firewall, or via another gateway (such as a frame relay connection). Identify all routes which traverse insecure networks.

Step 4: Verify that all network egress via insecure networks is encrypted via an authorized mechanism.

For firewall-routed traffic, verify whether the firewall is configured to route via VPN or to the internet.

```
# netstat –rn | grep 192.168.82
```

The route shown should be via the VPN DMZ interface, and not the internet DMZ interface.

Check the management interface on the VPN concentrator, and verify that the foreign networks are properly configured

Phase 2: Detect signs of unencrypted internet EPHI

Search for signs of unencrypted EPHI sent or received via the internet.

The following commands should be run on a network interface with full access to all internet traffic (only). An ethernet tap on the public interface of the internet firewall is the recommended method. A 'spanning port' with promiscuous access to all internet traffic also allowed: make sure the spanned port is full-duplex.

'ngrep' (Network Grep[7], a tool used to search for regular expressions in network traffic) is used in the following examples. See Appendix A for a detailed description of how these regular expressions were compiled. These commands assume the first interface is being used for packet captures. Use the '-d' flag to specify the correct interface if this is not the case.

Any network capture performed on a network containing EPHI may expose sensitive information, including EPHI. Do not perform these actions without consent of management.

Step 1: Search for signs of unencrypted HL7 internet traffic.

```
# ngrep –q "MSH\|\^\~\\\&" tcp
```

Step 2: Search for signs of unencrypted EDI HIPAA internet transactions.

```
# ngrep -q "\*004010X0(61|9[12345678])" tcp
```

Step 3: Search for signs of unencrypted Meditech internet traffic.

```
# ngrep –q ":\VMAGICDATA\"
```

Other steps: Search for signs of unencrypted EPHI in FTP data transfers

This command will search FTP data transfers for EPHI

```
# ngrep –qi "<string to search for>" port 20 and TCP
```

Replace <string to search for> with the appropriate string. The search is not case sensitive. Some suggested strings are:

- "*004010X0(61|9[12345678])"
- VMAGICDATA
- MSH\|\^\\\&
- lab results
- policy number
- Insurance eligibility
- Eligibility response
- Social security

See appendix C for other types of information to search for.

Other protocols such as SMTP (Simple Mail Transfer Protocol, aka email) or HTTP (Hypertext Transfer Protocol) may also be searched. The risk of 'false positive' matches will increase, as Electronic Health Information (not personally-identifiable, and thus not 'Protected', such as drug dosage information) are more likely appear in web and email traffic.

These commands will search email and web traffic respectively:

```
# ngrep –qi "<string to search for>" port 25 and TCP
# ngrep –qi "<string to search for>" port 80 and TCP
```

Phase 3: Verify HIPAA Security Awareness and Training

Verify that transmission security is part of GIAC Health's HIPAA Security Awareness and Training program (section 164.308 [a][5]). Ensure that employees and contractors of GIAC Health are properly educated regarding issues such as transmitting EPHI via insecure mechanisms, like email.

Appendix A – Capturing EPHI Packets

Many healthcare applications do not follow traditional protocol design, where a server is expected to listen on a well-known port (as described in /etc/services on Unix hosts), such as the telnetd server on TCP port 23.

The network protocols inspected for this paper (EDI/HIPAA transactions, HL7, and Meditech) did not adhere to a static server port choice. Traffic (both client and server) appeared on numerous ephemeral (1024 and above) TCP ports, and some applications also used UDP in addition to TCP.

This makes identification of networked EPHI more difficult. Network captures should inspect a wide range of ports (I recommend all ephemeral ports), in order to cast a wide enough net to capture relevant data.

A wide net raises the risk of false positives. The best approach may be to identify unique strings that are likely to appear only in the desired EPHI traffic. These strings are called 'regular expressions' (or 'regex') on Unix systems, and can be used with tools like ngrep.

Any network capture performed on a network containing EPHI may expose sensitive information, including EPHI. Ensure that any Intrusion Detection System complies with the HIPAA Security rule, and do not capture network traffic on a network used to transmit EPHI without consent of management.

Capturing Hl7 network traffic

HL7 stands for Health Level 7, a standard for transmitting Health Data. While all HL7 data is not necessarily EPHI (health data may not necessarily be 'protected'), there is a high likelihood that HL7 messages may contain EPHI.

Here is an example HL7 message, captured on a GIAC Health internal network:

```
MSH|^~\&|LAB|AB|EXAMPLELAB|EXAMPLELAB|20040525132614|AB01
2345|ACK|R|P|2.3||||.MSA|AA|R|HL7 ACK created
```

HL7 messages are transmitted via TCP, and appear to use random unprivileged port numbers. Any traffic analysis should examine all TCP ports 1024 and above.

Every HL7 message "without exception will contain exactly one MSH segment at its beginning"[8]. We will use this information to create a filter for monitoring unencrypted Hl7 transactions on the internet.

Following the initial MSH segment, the following characters usually appear in order: "|^~\&" They represent the suggested HL7 delimiters for field separator, component separator, repetition separator, escape character, and subcomponent separator, respectively.[9] Developers may use other delimiters, though this is rare in practice.

The majority of HL7 messages will begin with the string "MSH|^~\&". This regular expression matches that sequence (the additional backslash '\' characters are escape characters), and may be used with a tool like ngrep:

```
MSH\|\^\~\\\&
```

This will search TCP sessions for HL7 messages. Any such messages in internet traffic should be investigated.

Capturing HIPAA EDI network traffic

The HIPAA Transactions & Code Sets rule identifies the specific codes to be used in various medical transactions. These codes will appear in EDI transactions, and in unencrypted network captures of EDI transactions. We will use these codes as the basis for capturing unencrypted HIPAA transactions.

> 004010X061: Payroll Deducted and Other Group Premium Payment for Insurance Products
> 004010X091: Health Care Claim Payment/Advice
> 004010X092: Health Care Eligibility Benefit Inquiry and Response
> 004010X093: Health Care Claim Status Request and Response
> 004010X094: Health Care Services Review - Request for Review and Response
> 004010X095: Benefit Enrollment and Maintenance
> 004010X096: Health claim, institutional
> 004010X097: Health claim, dental
> 004010X098: Health Care Claim: Professional [10]

This regular expression matches those codes, and may be used with tools like ngrep:

```
004010X0(61|9[12345678])
```

EDI transactions may be transmitted via TCP. Tests show vendors use various unprivileged TCP ports for transmission, so any packet capture should use ports 1024 and above.

Here is a sample EDI packet containing a Health Care Eligibility Benefit Inquiry and Response EDI transaction. The HIPAA transaction code is highlighted in red.

```
ISA*00*          *00*          *AB*SAMPLE029   *ZZ*SAMPLE003
*040526*1253*U*00401*000000031*0*P*:.GS*HS*0000
0003R*SAMPLE003*20040526*1234*1*A*004010X092A1.ST*1232*12
34.BHT*0022*13* abc123456789012345678 9*20040526
*1253.HL*1**20*1.AB1*PR*2*SomeHospital*****PI*SAMPLE003.A
B*2*1*21*1.AB1*FA*2*GIACHealthcare*****SV*SAMPLE029.REF*N
7*AC -   Example Care
Center.HL*3*2*22*0.TRN*1*abc123456789012345678 9*99SAMPLE0
29.NM1*IL*1*DOE*JANE****MI*AB12345678900.ABC*D8*123456789
*F.EQ*30.XYZ*123*D8*20040526.AB*1234.CD*1*1.IEF*1*12.>>>.
```

Capturing Meditech network traffic

Meditech is a leading medical application vendor, and provides the primary medical application (also called “Meditech”) at GIAC Health.

Meditech servers use a range of ephemeral ports, and use both TCP and UDP packets. ALL TCP and UDP ports 1024 and higher should be searched.

Meditech network traffic contains medical transactions, and each message includes the full Windows pathname of the database used. GIAC Health’s databases are stored on applications servers under the E:\VMAGICDATA directory.

GIAC Health will use the regular expression “:\VMAGICDATA\” to search for signs of Meditech EPHI transmitted to the internet. In cases where the Meditech database is stored in another directory, change the “VMAGICDATA” string to that directory name.

Here is a sample Meditech network capture:

```
.\......C.+NEXT.AAAA.PATIENT.SAMPLE..E~.f........
O.5.E:\VMAGICDATA\ABC.UNIVERSE\ABC.LIVE.ABCD\ADM\
ABC\DATA\
```

Appendix B – HIPAA Policy Snort IDS signatures

These signatures are designed to detect unencrypted EPHI; they may prove useful on a snort sensor sniffing internet traffic. They should not be used on internal sensors where unencrypted network EPHI is expected.

Any network capture performed on a network used to transmit EPHI may expose sensitive information, including EPHI. Make sure that any Intrusion Detection System complies with the HIPAA Security rule, and do not capture network traffic on a network used to transmit EPHI without consent of management.

These signatures have been tested on the Snort Intrusion Detection System, version 2.1.2 (see http://www.snort.org)

```
alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HL7 message";
content:"|0B4D53487C5E7E5C26|"; depth:50; flags:A+;
classtype: policy-violation; sid:1000000; rev:1;)

# You may need to change the string 'VMAGICDATA' to the
# root directory of your Meditech database
alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted Meditech TCP traffic";
content:"VMAGICDATA"; depth:100;  flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)

alert udp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted Meditech UDP traffic";
content:"VMAGICDATA"; depth:100; classtype: policy-
violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Payment for Insurance
Products)"; content:"004010X061"; flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health Care Claim
Payment/Advice)"; content:"004010X091"; flags:A+;
classtype: policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health Care
Eligibility Benefit Inquiry and Response)";
content:"004010X092"; flags:A+; classtype: policy-
violation; sid:1000000; rev:1;)
```

```
alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health Care Claim
Status Request and Response)"; content:"004010X093";
flags:A+; classtype: policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health Care Services
Review)"; content:"004010X094"; flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Benefit Enrollment and
Maintenance)"; content:"004010X095"; flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health claim,
institutional)"; content:"004010X096"; flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health claim,
dental)"; content:"004010X097"; flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)

alert tcp $HOME_NET 1024: <> $EXTERNAL_NET 1024:
(msg:"Unencrypted HIPAA Transaction (Health claim,
professional)"; content:"004010X098"; flags:A+; classtype:
policy-violation; sid:1000000; rev:1;)
```

Appendix C – The 18 Protected Health Information Identifiers

The HIPAA privacy rule lists 18 identifiers make PHI personally-identifiable, and thus 'protected'. If all eighteen are removed, the PHI is no longer 'protected', and no longer subject to HIPAA privacy rule.

These identifiers, while not part of the HIPAA Security rule, can be used as a checklist for detecting EPHI.

This list is taken from the final HIPAA Privacy Rule, section 164.514.[11] Link: http://www.hhs.gov/ocr/combinedregtext.pdf

(A) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
(B) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(C) Telephone numbers;
(D) Fax numbers;
(E) Electronic mail addresses;
(F) Social security numbers;
(G) Medical record numbers;
(H) Health plan beneficiary numbers;
(I) Account numbers;
(J) Certificate/license numbers;
(K) Vehicle identifiers and serial numbers, including license plate numbers;
(L) Device identifiers and serial numbers;
(M) Web Universal Resource Locators (URLs);
(N) Internet Protocol (IP) address numbers;
(O) Biometric identifiers, including finger and voice prints;
(P) Full face photographic images and any comparable images; and
(Q) Any other unique identifying number, characteristic, or code; and

References

[1] HIPAA Security Final Rule, Federal Register Volume 68 No 34, section 164.312, page 8379.
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

[2] ibid

[3] ibid, section 160.103, page 8374

[4] ibid, page 8357

[5] ibid, page 8357

[6] "Boiler-plate" policy text based on SANS sample policies, such as:
http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf

[7] Network grep: http://ngrep.sourceforge.net/
Ngrep is available for Windows and Unix

[8] "Other Standards in the Healthcare Industry -HL7"
http://freehost04.websamba.com/dicom4india/OtherStd.htm

[9] From "Additional Implementation Message Guide", HL7 Version 2.4 Standard, Release 1.0, Health Level Seven, Inc. Page 21, Section 314, "Message Delimiters". http://www.hl7.org/Special/committees/claims/HL7ClmAttIG.PDF

[10] HIPAA Transactions & Code Sets
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/finalrule/txfin01.asp

[11] Final HIPAA Privacy Rule, section 164.514.
http://www.hhs.gov/ocr/combinedregtext.pdf