# Location of digital signatures in healthcare messaging

<table>
<thead>
<tr>
<th>Part Title:</th>
<th>Click here and type Part Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designation:</td>
<td>HB</td>
</tr>
<tr>
<td>Part Number:</td>
<td>Click here and type Part Number (do not include the word PART)</td>
</tr>
<tr>
<td>Supersedes Standard No:</td>
<td>Click here and type Superseded Standard Number</td>
</tr>
<tr>
<td>AustralianORJoint:</td>
<td>Australian</td>
</tr>
<tr>
<td>Creation Date:</td>
<td>2006-11-21</td>
</tr>
<tr>
<td>Revision Date:</td>
<td>Enter date in YYYY-MM-DD format (essential when posting to web)</td>
</tr>
<tr>
<td>Issue Date:</td>
<td>November 2006</td>
</tr>
<tr>
<td>Committee Number:</td>
<td>IT-014</td>
</tr>
<tr>
<td>Committee Title:</td>
<td>Health Informatics</td>
</tr>
<tr>
<td>Subcommittee Number:</td>
<td>IT-014-06</td>
</tr>
<tr>
<td>Subcommittee Title:</td>
<td>Messaging</td>
</tr>
<tr>
<td>Project Manager:</td>
<td>Elizabeth Hanley</td>
</tr>
<tr>
<td>PMs Email Address:</td>
<td><a href="mailto:Elizabeth.Hanley@standards.com.au">Elizabeth.Hanley@standards.com.au</a></td>
</tr>
<tr>
<td>WP Operator:</td>
<td>Denisa</td>
</tr>
<tr>
<td>Project Number:</td>
<td>6996</td>
</tr>
<tr>
<td>Combined Procedure?:</td>
<td>No</td>
</tr>
<tr>
<td>Committee Doc No.:</td>
<td>ONE Alpha followed by FOUR numerical (eg: N9999)</td>
</tr>
<tr>
<td>Stage:</td>
<td>PRELIMINARY</td>
</tr>
</tbody>
</table>
Committee Reps:  
Australian and New Zealand College of Anaesthetists
Australian Association of Pathology Practices
Australian Electrical and Electronic Manufacturers Association
Australian Health Care Association
Australian Health Insurance Association
Australian Healthcare Association
Australian Information Industry Association
Australian Institute of Health & Welfare
Australian Institute of Radiography
Australian Medical Association
Australian Private Hospitals Association
Central Queensland University
Commonwealth Department of Health and Aging
Consumers’ Federation of Australia
Consumers’ Health Forum of Australia
CSIRO e-Health Research Centre
Department of Health (South Australia)
Department of Health Western Australia
Department of Human Services, Victoria
Engineers Australia
General Practice Computing Group
Health Informatics Society of Australia
Health Information Management Association of Australia
Health Professions Council Of Australia
HL7 Australia
Medical Industry Association of Australia
Medical Software Industry Association
Medicare Australia
National Health Information Management Group
NSW Health Department
Pharmaceutical Society of Australia
Pharmacy Guild of Australia
Queensland Health
Royal Australian and New Zealand College of Obstetricians and Gynaecologists
Royal Australian and New Zealand College of Radiologists
Royal Australian College of General Practitioners
Royal Australian College of Medical Administrators
Royal College of Nursing, Australia
Royal College of Pathologists of Australasia
Society of Hospital Pharmacists of Australia
University of Sydney

Additional Interests:  
Buderim Gastroenterology Centre
Cerner Corporation
Collaborative Centre for eHealth
DH4
General Practice Computing Group
HCN
La Trobe University
McCaulley Software
Michael Legg & Associates
Ocean Informatics
Pen Computer Systems

Product Type:  
HB

Document Status:  
Current

Document Availability:  
Private

Final Publication

Date Approved:  
Click here and type Date approved
PREFACE

The Electronic Transactions Act (ETA) 1999 sets out the IT standards that Medicare Australia (MA) requires for the electronic transmission, and storage of documents to approved practitioners. This legislation requires that the Document:

(a) consists of a standard e-mail message or a recognized Electronic Data Interchange (EDI) format that is transmitted using Public Key Infrastructure (PKI) standards; and

(b) be digitally signed by the requesting practitioner using an individual private key for which there is a current public key Certificate to allow a practitioner to verify the authenticity of the document upon receipt.

This document—Handbook outlines one such ‘recognized EDI format’ that is recommended for use throughout messaging in Australia, along with a standard method for encoding this signature in a Health Level Seven (HL7) message.

Standards Australia wishes to thank the Department of Health and Ageing for their continued financial support in helping us to achieve our aims.
## CONTENTS

<table>
<thead>
<tr>
<th>SECTION 1  SCOPE</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 GENERAL</td>
<td>4</td>
</tr>
<tr>
<td>1.2 PURPOSE</td>
<td>4</td>
</tr>
<tr>
<td>1.3 BENEFITS</td>
<td>4</td>
</tr>
<tr>
<td>1.4 TARGET USERS</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECTION 2  TERMS AND DEFINITIONS</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 DEFINITIONS</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECTION 3  OVERVIEW</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 WHAT ARE DIGITAL SIGNATURES?</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECTION 4  HL7 MESSAGES</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 DIGITAL SIGNATURES IN HL7 MESSAGES</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APPENDIX A</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>26</td>
</tr>
</tbody>
</table>
SECTION 1  SCOPE

1.1 GENERAL
The Australian Government’s Electronic Transactions Act and equivalent State and Territory Act’s allows where stated for paperless digitally signed documents to be implemented in place of physically signed paper documents.

For auditing or archiving purposes, it is essential that the digital signature on a transaction/document can be verified at anytime.

1.2 PURPOSE
This paper puts forward two methodologies for attaching the digital signature to a health sector electronic transaction so that they are intrinsically linked. It is not proposed to develop new material but to review a range of existing industry security guidelines on this topic and to recommend a limited set of options applicable to the various communication channels available over the Internet.

The publication will address messaging standards HL7 V2.

1.3 BENEFITS
Digital Signatures in Healthcare Messaging offer a range of benefits. It enables users to know:

(a) Who sent the message (authentication).
(b) The message content has not been altered in any way between sending and receiving (integrity).
(c) The sender cannot at some later stage dispute they created and sent the message (non-repudiation).
(d) That only the person the message is directed to can open it (confidentiality).
(e) Reduced risk of errors.
(f) Better quality of written information – no difficulty reading handwriting.
(g) Efficiencies for the provider in the single entry of data into a clinical information system.
(h) The automatic generation of the document by the clinical information system.
(i) A speedy exchange of information to ensure that consumer needs are more quickly addressed.
(j) Health professionals are released from the burden that paper information and paper work has created, enabling them to spend more time directly addressing consumer needs.
(k) Confidentiality and security of consumer information will be improved, as access will be on a ‘need to know’ basis only.
1.4 TARGET USERS

This document is intended for clinicians and practitioners in the public and private health and welfare sectors, ranging from allied health clinicians, ancillary health practitioners, general practitioners, pharmacists, specialists, and surgeons. It also targets software developers, state health and human services departments, NEHTA, health informatics consultants and software vendors, consumers and academics. It contains information that should help all of these parties better understand the methodologies for attaching the digital signature in a health sector electronic transaction.
# SECTION 2 TERMS AND DEFINITIONS

## 2.1 DEFINITIONS

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signature</td>
<td>A digital signature is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged.</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange is the inter-organizational, computer-to-computer exchange of structured information in a standard, machine-processable format.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The process of converting data into a form or code that cannot be understood by unauthorized persons.</td>
</tr>
<tr>
<td>ETA</td>
<td>Electronic Transactions Act 1999</td>
</tr>
<tr>
<td>Hash</td>
<td>A hash value, also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.</td>
</tr>
<tr>
<td>HL7</td>
<td>Health Level Seven is a specification for a health data-interchange standard designed to facilitate the transfer of health data resident on different and disparate computer systems in a health care setting. HL7 facilitates the transfer of laboratory results, pharmacy data and other information between different computer systems.</td>
</tr>
<tr>
<td>Key</td>
<td>A variable value created using a mathematical formula. Public keys are obtained from the certificate authority, while private keys are contained within each user’s computer system (also see Public Key).</td>
</tr>
<tr>
<td>MA</td>
<td>Medicare Australia</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5. MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size.</td>
</tr>
<tr>
<td>Metadata</td>
<td>A description of data</td>
</tr>
<tr>
<td>Private key</td>
<td>A mathematically-derived code provided by a certificate authority. The private key is stored in the user’s computer and is not accessible to the public. It can be combined with the public key to encrypt and decrypt messages.</td>
</tr>
<tr>
<td>Public key</td>
<td>A mathematically-derived code provided by a certificate authority. The public key is stored in the digital certificate and can be combined with the private key to encrypt and decrypt messages.</td>
</tr>
<tr>
<td>Public key infrastructure (PKI)</td>
<td>A software application that allows users to encrypt and send information securely over a public network (also see encryption).</td>
</tr>
<tr>
<td>Repository</td>
<td>Database of information about source and target applications that includes data elements, inputs, processes, outputs, and relationships between applications.</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SHA1</td>
<td>Secure Hash Algorithm 1 takes a message of less than 264 bits in length and produces a 160-bit message digest designed so that it is computationally very expensive to find a text string that matches a given hash.</td>
</tr>
<tr>
<td>XML</td>
<td>A flexible language for creating common information formats and sharing both the format and the data on the World Wide Web and elsewhere. XML, a formal recommendation from the World Wide Web Consortium (W3C), is similar to the language of today’s Web pages, the Hyper Text Markup Language (HTML).</td>
</tr>
</tbody>
</table>
SECTION 3 OVERVIEW

3.1 WHAT ARE DIGITAL SIGNATURES?

A Digital signature is a method of signing an electronic document that identifies and authenticates a particular person as the source of the electronic document and indicates that persons approval of (and accountability for) the information contained in the electronic document. A number of technical solutions for the use of digital signatures have been identified and evaluated, with PKI being the Australian Government preferred solution.

PKI is a trusted framework adopted by Australian Government to provide authentication and confidentiality for online transactions through the use of digital keys and certificates. For the healthcare sector, PKI enables the transfer of sensitive medical information across the Internet, without compromising the individual’s right to privacy.

PKI digital certificates may be issued to an organization (‘location certificates’) or to an individual (‘Individual Certificates’). Location certificates allow a number of people at the same location to sign, encrypt and exchange messages electronically with other certificate subscribers. The location certificate provides confidentiality, authentication, and integrity of the information that is transmitted. Signing a message using the location certificate confirms the location that the message came from, but not from which individual. Individual certificates are specific to an individual and are used to sign, encrypt and exchange messages electronically with other certificate subscribers. Individual certificates provide authentication, confidentiality, integrity and non-repudiation.

Ideally, the electronic exchange of information should utilise individual certificates for signing because:

(a) a valid document must unambiguously identify the implementer as the signer of the document; and

(b) a document may contain personal and potentially sensitive information.

However the anecdotal evidence suggests that, in practice the implementation of individual certificates over location certificates, has been problematic. Therefore, the implementation of digital signatures using PKI requires careful consideration of the practical issues surrounding the use of individual and location certificates in the Healthcare sector. One possibility might be that PKI location certificates are used in combination with another method of authentication, e.g. username and password, underpinned by legal or policy frameworks.

A digital signature has the same legal holding as your hand written signature. This was introduced in the Commonwealth Electronic Transactions Act in 1999.
The hash algorithm creates a unique abstract of the message

Private key of sender encrypts digest

Message

Hash function

Message digest

Digital signature

Digital signature

Encrypted digest becomes digital signature

FIGURE 1  OVERVIEW OF A DIGITAL SIGNATURE PROCESS
SECTION 4 HL7 MESSAGES

4.1 DIGITAL SIGNATURES IN HL7 MESSAGES

4.1.1 Proposed methodology 1

4.1.1.1 Overview

The goal of this methodology is to attach the digital signature to the electronic message, with the relevant information included in the message to verify the digital signature at any time. It is essential that the digital signature is stored with the message. It is intended that the signature is attached to the message without impacting on the data processing. Thus all software should still be able to successfully parse the message, without needing to know there is a digital signature attached.

The Electronic Transactions Act 1999 states:

‘Where a medical practitioner:

(a) refers a patient to a specialist or consultant physician; or
(b) requests a pathology service; or
(c) requests a diagnostic imaging service, by electronic means,

MA requires that the referral or requests:

(i) consist of either a standard e-mail message, or a recognized EDI format, that is transmitted using PKI standards;
(ii) meet all the requirements for a Referral or Request provided in the Act, the regulations and the MA (PKI Standards) regulations; and
(iii) be digitally signed by the referring/requesting practitioner using an individual private key for which there is a current public key certificate recognized by MA (in accordance with PKI standards), to allow a specialist, consultant physician, or Approved Pathology Practitioner or medical practitioner to verify the authenticity of the Referral or Request upon receipt.’

While individual messages can be signed, it makes batch transmission and passage through interface engines very difficult unless the message is sent as a single message and the whole message is archived. This also means that being able to verify the authenticity of a message requires this file to be made available.

One approach is to embed the signature in the message so that only the data in the message was required to verify the authenticity at any stage in the future. By using standard structures already in the standard this data could reside in a message and be ignored if verification was unavailable or not desired. Old applications would simply process the data in the standard way without being able to interpret it but without the need for any changes. The data remains available for later use then.

From the point of view of the doctor and MA the important data is content of the message, who it was on, and what date it was created. Data, such as name data is volatile over time and should be encapsulated within the message so that the document can be sent under e.g. a married name without invalidating the signature.

This is a tested and proven schema to accomplish this process. It covers PKI signatures and MD5 and SHA1 hashes. Hashes do not meet the ETA requirements but may be useful when you wish to protect the integrity of the data for other reasons.
4.1.1.2 HL7 Version 2

The first option being explored for HL7 Version 2 was intended as a solution for Pathology reports* only, but can work for all HL7 Version 2 messages using an observation (OBX) segment. This solution could make OBX segments mandatory in all messages to be signed.

The basic algorithm to attach the signature in HL7 Version 2 is to add two OBX segments to the end of an ORU message. The first added OBX uses an FT (freetext) datatype and contains the important PID and OBR data such as the patient name, the test name and the date of the test. This can be extended at will as it has to be generated prior to signing the message and its actual content is not critical, basically whatever data you wish to preserve over time. The second OBX contains the actual signature data, e.g. in the case of PKI it is encapsulated in an ED data type in this OBX segment. What is actually signed is all the data in the OBX segments above the last OBX segment.

As an example, here is a simple unsigned pathology message:

```
MSH|^~\&|TEST^TESTAPP^L|Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||20040410141133||ORU^R01...

PID|1|||PATIENT^Test^^^^^^L||20000101|||139 King Street^^BUDE...'

PV1|1|O|||0341615J^WHITE^MELISSA^^^DR^^AUSHICPR^L^^UPIN|0341615J^WHITE^MELISSA^^^DR^^AUSHICPR^L^^UPIN|||N

ORC(CE)|F71DEE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||CM|||0341615J^WHITE^MELISSA^^^DR^^AUSHICPR^L^^UPIN

OBX|1|FT|28655-9||This a simple ^H<Test Message^N To demonstrate signing a...

OBX|2|SN|5048-4^ANA titre^LN||<^40|titre|||F
```

Here is the same message signed by a PKI key:

```
MSH|^~\&|TEST^TESTAPP^L|Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||20040410141133||ORU^R01...

PID|1|||PATIENT^Test^^^^^^L||20000101|||139 King Street^^BUDE...'

PV1|1|O|||0341615J^WHITE^MELISSA^^^DR^^AUSHICPR^L^^UPIN|0341615J^WHITE^MELISSA^^^DR^^AUSHICPR^L^^UPIN|||N

ORC(CE)|F71DEE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||CM|||0341615J^WHITE^MELISSA^^^DR^^AUSHICPR^L^^UPIN

OBX|1|FT|28655-9||This a simple ^H<Test Message^N To demonstrate signing a...

OBX|2|SN|5048-4^ANA titre^LN||<^40|titre|||F
```

* IT/14/6/5 Andrew McIntyre, ‘Pathology Signature Document’ [email dated 5 Nov 2004]
Grahame Grieve, ‘Pathology request Electronic Signature in HL7’ [email dated 24 March 2004]
OBX segments 3 and 4 have been added. OBX 3 is simply to store relevant ORC/OBR/PID data that needs to be signed. An application that doesn't understand the signature should still cope with these segments.

What are extracted are all the fields in OBX that affect display. The reason for doing it this way is to overcome problems with errors in formatting (e.g. unneeded Field separators) that may be in the original message and to allow any system that stores the data to reconstruct this at will so the signature can be validated at any time. There is no requirement that the data stay in HL7 format, just that the data is preserved and available. XML and classic encoding can be translated freely and still have a valid signature.

A similar process could be used for pathology orders. What was ordered and who it was ordered by can be added to the SIGNATURE_HEADER and an OBX added to the order message to sign this data. Then you can "verify the authenticity of the Referral or Request" at any time. The signature data can be stored in the same way existing data is stored.

The required Identifiers are:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSHICPKI</td>
<td>To indicate that this is a MA PKI signature — used in ED segment – Namespace ID.</td>
</tr>
<tr>
<td>AUSETAV1</td>
<td>To indicate that this OBX contains PKI signature data — should have a version number to indicate algorithm (ED Segment).</td>
</tr>
<tr>
<td>AUSSHA1HASH</td>
<td>To indicate that this is a SHA1 hash of the message (Base 64 encoded in ST segment as short).</td>
</tr>
<tr>
<td>AUSMD5HASH</td>
<td>To indicate that this is a MD5 hash of the message (in ST segment as usually Hex encoded).</td>
</tr>
</tbody>
</table>

Example files are included that show the 3 variations in Table 1. The original message is in TestPatient.oru (see Appendix A.1).

### TABLE 1

<table>
<thead>
<tr>
<th>File Name</th>
<th>Signature Algorithm</th>
<th>What was signed</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestpatientETA.oru</td>
<td>PKI Signature (ED Datatype)</td>
<td>SDataETA.txt</td>
</tr>
<tr>
<td>TestpatientMD5.oru</td>
<td>MD5 hash (ST Datatype)</td>
<td>SdataMD5.txt</td>
</tr>
<tr>
<td>TestPatientSHA1.oru</td>
<td>SHA1 hash (ST Datatype)</td>
<td>SDataSHA1.txt</td>
</tr>
</tbody>
</table>

4.1.1.3 The algorithm

The algorithm treats each OBX in a standard way, each data type has to be treated differently but every field is separated by a ‘.’ (Full stop) and each OBX segment by a <CR><LF> sequence. If a field is blank then the full stop is still written. A few fields of some data types have been omitted, usually because of optional, non critical values in these fields. In general ST, FT and SN data types will cover 99% of the information but it is possible to encode any data type. The order of the fields in the methodology is used
to write the values; however, there is an exception, which is the Observation value in OBX. This is written last for every OBX.

Pseudo code for this is detailed below.

Build a string to sign or hash.

For each OBX in order add these values (include SIGNATURE_HEADER OBX).

\{
    OBX.Value_Type
    .
    OBX.Observation_Identifier.Identifier
    .
    OBX.Observation_Identifier.Text
    .
    OBX.Observation_Identifier.NameOfCodingSystem
    .
    OBX.Observation_SubID
    .
    OBX.Units.Identifier
    .
    OBX.Units.Text
    .
    OBX.Units.NameOfCodingSystem
    .
    OBX.References_Range
    .
    for each OBX.Abnormal Flags
        OBX.Abnormal_Flag[i]
    .
    OBX.Status <- or 'F' if blank
    .
    OBX.Date_Of_Observation
    .
    Then add all field values for Result values

Depends on value type but for example
  SN - Structured Numeric
      SN.Comparator
      .
      SN.Num1
      .
      SN.Separator
      .
      SN.Num2
      .
  Now add <CR><LF>
\}

Now check or create detached signature/hash on resulting string.

OBX Value Type Handling

SN as above

FT/ST/DT/TS

For each observation value
  Add Text
  Add '.'
These are less common but could appear.

XCN

For each observation value
  Add IDNumber
  Add '.
  Add FamilyName
  Add '.
  Add GivenName
  Add '.
  Add MiddleName
  Add '.
  Add Suffix
  Add '.
  Add Prefix
  Add '.

XPN

For each observation value
  Add FamilyName
  Add '.
  Add GivenName
  Add '.
  Add MiddleName
  Add '.
  Add Suffix
  Add '.
  Add Prefix
  Add '.

ED

For each observation value
  Add SourceApplication.NameSpaceID
  Add '.
  Add SourceApplication.UniversalID
  Add '.
  Add SourceApplication.UniversalIDType
  Add '.
  Add MainTypeData
  Add '.
  Add DataSubType
  Add '.
  Add Encoding
  Add '.
  Add Data
  Add '.

RP

For each Observation value
  Add Pointer
  Add '.
  Add TypeOfData
  Add '.
  Add ApplicationID.NameSpaceID
  Add '.'
Add ApplicationID.UniversalID
Add '.
Add ApplicationID.UniversalIDType
Add '.
Add SubType
Add '.

EI

For each Observation value
Add EntityIdentifier
  '.
  Add NameSpaceID
  '.
  Add UniversalID
  '.
  Add UniversalIDType
  '.

4.1.2 Proposed methodology 2

4.1.2.1 Overview

This methodology describes a process for signing a document by a practitioner when a document is created. This single signed document is both human readable, and machine parsable. This signed document stands alone from any particular message format, and can be stored in a database by any system.

This methodology describes the format of this signed document. A signed document actually consists of 3 parts, the signed document, the electronic signature, and some metadata describing the contents of the signed document.

This methodology also describes how a signed document can be embedded in an HL7 message for transmission between the system representing the requesting practitioner and the approved provider, and then potentially used in referrals between multiple providers.

From the messaging perspective, the document is treated as signed persistent data. Rather than applying the digital signature process to a particular message, a specific representation of the document is signed, and this representation is attached to a message.

Signing a specific representation of the document, rather than the message being transmitted between systems, results in the document decoupling from the requesting/signing and messaging process, resulting in many advantages, such as:

(a) The user sees and understands what is signed.

(b) Messages may be generated by processes separated from the user by time and space.

(c) Messages concerning the document may be retransmitted from the requesting system to the provider system, or from one provider system to another if required.

(d) Messages may be modified in transmission without invalidating the document and signature. Modification of messages is often required in real world situations. There is more complete discussion of this issue below.

(e) The signed document can be stored in a database without requiring full storage of the message.
4.1.3 The signable document

The Signable Document is a simple format that encapsulates the essence of the order in a single format that can be read by both non-technical humans and machines, and signed as is with no manipulation.

The Signable Document takes the form of a series of name/value pairs. The following names must be contained in the Signable Request.

<table>
<thead>
<tr>
<th>Name</th>
<th>Format</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider ID; Name</td>
<td>ID; Name</td>
<td>ID: The Full provider number issued by MA. This must be the Provider number by which the document is made, and must be the Provider number registered against the MA key by which the request is signed. Name: The legal name of the practitioner identified by the provider number. There is no constraints on the form of this name – it is not intended to be machine readable. Both ID and Name are required.</td>
</tr>
<tr>
<td>Patient ID</td>
<td></td>
<td>The ID(s) by which the patient is known. Multiple ID’s are allowed. Each ID has the form ‘INST ID’ where INST is an alphanumeric code that identifies the identifier and the ID is the identifier itself. The INST ‘MA’ is reserved for the Medicare number, and the Medicare number should always be included in this list. The Full representation of the INST for a given code can be found in the meta data section.</td>
</tr>
<tr>
<td>Patient Name</td>
<td></td>
<td>The legal name of the patient as found on the Medicare card. The preferred form of the name is exactly that found on the Medicare Card.</td>
</tr>
<tr>
<td>Patient DOB</td>
<td>DD MMM CCYY</td>
<td>The DOB of the patient. Where the date of birth is unknown, or known to less precision than the format allowed, the Value ‘U’ should be used.</td>
</tr>
<tr>
<td>Request Date</td>
<td>DD MMM CCYY HH:NN:SS</td>
<td>The Date that the document was made. This date must be able to be used as a uniqueness marker. Systems generating signed documents must ensure that the combination of document provider and Document date is unique.</td>
</tr>
<tr>
<td>Requests</td>
<td></td>
<td>A list of investigations requested. Multiple Items are allowed. The Code set used for the Requests is defined in the metadata.</td>
</tr>
<tr>
<td>Service</td>
<td>ID; Name</td>
<td>ID: The NATA number for the intended service. Name: The legal name of the intended service. Both ID and Name are required.</td>
</tr>
</tbody>
</table>

All of these are required, that is, each of these must be in the Signable Document, and must contain a non-null value. The values can be included in any order.

Encoding a signable document

A Signable Document must be encoded in precisely the fashion described in this section.

The Signable Document is encoded in UTF-8 (W3C-XML-Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/) Each Name/Value pair is separated by the UTF-8 characters #13#10. Each Name/Value Pair is encoded in the following fashion: The Name, followed by the character pair ‘:’, then the value. No trailing spaces
are allowed. Where multiple items are allowed in the value, they are separated by the character pair ‘,’.

Example:

Provider: 045678AB; Dr John Handy
Pathology: NATA1234; Acme Pathology
Patient ID: SURG P00057804, MA 4009887514
Patient Name: ALAN R SMITH
Patient DOB: 21 Jun 1977
Request Date: 12 April 2000 08:08:33
Requests: VAN, GAM, FBC, HAB

Signing the document

It is anticipated the actual Document in the encoded format specified above will be shown to the practitioner at the time the request is signed. The signing process will generate a digital signature. The document and the digital signature should be stored in accordance with MA storage requirements outlined in the ETA.

The document metadata

This section contains data that may be required to assist systems to understand the request, but is not part of the actual request itself. In general, this information would not change between requests. This information must be transmitted with the document to ensure ready availability.

The metadata consists of a series of name/value pairs. The following names are defined.

<table>
<thead>
<tr>
<th>Table 3</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Optionality</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Required</td>
<td>Information relating to the software that generated and encoded the signable document. This must identify the vendor of the software. Release or version numbers are recommended.</td>
</tr>
<tr>
<td>Institution</td>
<td>1 for each INST used in request</td>
<td>ID; Information ID is the INST used in the signable request. Information identifies the institution. &lt;what goes here?&gt;</td>
</tr>
<tr>
<td>Request Codes</td>
<td>Optional</td>
<td>Request code set used for requests. Values must be taken from this table: AUS Request codes published by Standards Australia MBS MBS codes The default value is AUS.</td>
</tr>
</tbody>
</table>

Example:

System: Acme Inc; GP system V1.02.003 (Cust 1002)
Institution: SURG; ?
Request Codes: AUS

Encoding the signable document in an HL7 message

The Signable Document, digital signature, and metadata, must be included in any order message that is sent to a filler system. HL7 has not provided any mechanism to associate persistent signed data with a particular order or set of orders. This feature has
been requested, but it is not clear whether this will become part of the version 2 messaging framework. In the interim, until a properly modelled solution is available, the method described here can be used.

A message may contain only one signature. The signed document must include all of the request items placed in the message. Not all the items requested in the signed document need be requested in the message. (This is particularly relevant for inter-pathology referrals).

There are 4 proposed solutions for attaching this information to a document (Options: #1, #2, #3 and #4).

4.1.3.1 Option #1 – use of NTE segment

The Signature is considered to be a note attached to the message. The Signable Document, its signature and metadata are encoded in a series of NTE segments after the MSH segment, as described in the segment structure for HL7 order messages.

The NTE segment has the following fields:

<table>
<thead>
<tr>
<th>SEQ</th>
<th>LEN</th>
<th>DT</th>
<th>REP</th>
<th>TBL#</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>SI</td>
<td></td>
<td>Set ID - NTE</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>ID</td>
<td></td>
<td>Source of Comment</td>
</tr>
<tr>
<td>3</td>
<td>64k</td>
<td>FT</td>
<td>Y</td>
<td>Comment</td>
</tr>
<tr>
<td>4</td>
<td>250</td>
<td>CE</td>
<td></td>
<td>Comment Type</td>
</tr>
</tbody>
</table>

The 3 NTE segments are built as follows:

<table>
<thead>
<tr>
<th>Segment</th>
<th>NTE-2</th>
<th>NTE-3</th>
<th>NTE-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>Request with each name value pair as a repeat (replace #13#10 with ~)</td>
<td>ETAREQ^^HL70364</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td>Base64 Encoded Signature, with each line as a repeat</td>
<td>ETASIG^^HL70364</td>
<td></td>
</tr>
<tr>
<td>Metadata</td>
<td>Meta with each name value pair as a repeat (replace #13#10 with ~)</td>
<td>ETAMETA^^HL70364</td>
<td></td>
</tr>
</tbody>
</table>

The vocabulary for HL7 Table 364 has been extended with the 3 codes above.

An example message would look like this:

```
MSH|\~\&|PMSX21|GX3261|QMLPTX|QML^2184^AUSNATA|200004120817||
ORM^O01^ORM_O01|
GX3261_20000412-2.211|P|2.3.1|2173||AL||AU
NTE|O|Provider: 045678AB; Dr John Handy~Pathology: NATA1234; Acme Pathology~Patient ID: SURG P00057804, MA 4009887514~Patient Name: ALAN R SMITH~Patient DOB: 21 Jun 1977~Request Date: 12 April 2000 08:08:33~Requests: VAN, GAM, FBC, HAB|ETAREQ^^HL70364
```
This example is based on an example taken from HB 262 the handbook for pathology messaging. The example signature is not valid.

Possible Concerns with Option #1:

(a) Use of NTE when NTE is not a preferred segment in Australian Standards.
(b) The creation of new codes for the NTE and choice of description of the code set.

4.1.3.2 Option #2: use MSH-8

MSH-8 is the otherwise undescribed security field in MSH. This option regards the signature information as message security information.

The following rules are to be followed when generating the content of the MSH-8 field:

(a) Append the Metadata to the request, separating them with an extra #13#10.
(b) Append the signature (in binary format) to this, separating it with an extra #13#10.
(c) Base64 encode this.
(d) Remove any #13 or #10 characters in the base64 encoded output.

This description would be formalised if Option #2 is preferred.

This is the content of the MSH-8 field. The length of this is going to exceed the allowable length of MSH-8 in the HL7 standard.
Here is an example message:

```
MSH|^~\&|PMSX21|GX3261|QMLPTX|QML^2184^AUSNATA|200004120817|
UHJvdmlkZX16I

DA0NTY3OEFCOyBEciBKb2hulEhhbmr5DQpQYXRb2xvZ3k6IE5BVEExMjM0OybBY211IFBhd

GhvBG9neQ0KUGF0aWVudCBJRDogU1VSRyBQMDAwNTc4MDQsIEhJQyA0MDA5ODg3NTExDQpQY

XrpZW50IE5hbWU6IEFMQMU4gUiBITTuUlUSA0KUGF0aWVudCBET0I6IExIXEp1biAxOTc3DQpQSZ

XF1ZXN0IERhdGU6IEFwcmlsIG1wMDAwMDg6MDg6MzMCIJlcXVlc3RzOIBQU4sIEdBT

SwgRkJDLCB3Qg0KU3lzdGVtOiBBY211IEluYzsgR1Agc3lzdGVtIFBYxLjAyLjAwMyAoQ

3VzdCAxMDAyKQ0KSW5zdGl0dXRpb246IFNVUkc7ID8NClJlcXVlc3QgZmF6IjEh
```

```
acTudbm3CEi8dfjvORM^O01^ORM_O01|GX3261_20000412-
2.211|P|2.3.1|2173||AL||AU

PID|1||P00057804|~--4009887514|MC~SMIAL001|SR||SMITH^Alan
n^Ross^^Mr||

19770621|M|818 Beach Road^^BEECHMERE|^4510^AU^H|||4097859602

PV1|1|1|045678AB^HANDY^JOHN^Dr|045678AB^HANDY^JOHN^Dr

ORC|NW|173-0^GX3261||173^GX3261|IP||045678AB

OBR|1|173-0^GX3261||VAN^VANCOMYCIN(PRE/POST),S^NATA2184-
```

```
2|||||||045678AB^HANDY^JOHN^Dr\00004120817^^R

ORC|NW|173-1^GX3261||173^GX3261|IP||045678AB

173-1^GX3261||GAM^IMMUNOGLOBULINS,SERUM^NATA2184-2
```

```
4|||||||045678AB^HANDY^JOHN^Dr\00004120817^^R

ORC|NW|173-2^GX3261||173^GX3261|IP||045678AB

OBR|3|173-2^GX3261||FBC^FULL BLOOD EXAMINATION^NATA2184-
```

```
4-1|||045678AB^HANDY^JOHN^Dr\00004120817^^R\0321654B^R

ORC|NW|173-3^GX3261||173^GX3261|IP||045678AB

OBR|4|173-3^GX3261||HAB^HEPATITIS A \T\ B ACUTE^NATA2184-
```

```
1-1|||0321654B^R
```
```
This is the same example as in option #1.

Concerns with Option #1:

(i) Use of MSH-8 prevents any other use of MSH-8.
(ii) Field length will be longer than expected in the standard.
(iii) Field is poorly described and marked up (more detail could be added to the field contents but this is of dubious value).

### 4.1.3.3 Option #3: use OBX

In option #3 the request is considered to be an observation concerning the order, and is encoded in an OBX segment. There is a logical problem here, which is that the request may be spread across multiple ORC/OBR pairs, and each of these contains multiple OBX segments. This methodology recommends that the signature be attached to the first ORC/OBR pair. There would be 3 OBX segments, for the request, the signature, and the metadata.

The 3 OBX segments are built as follows:

#### TABLE 6

<table>
<thead>
<tr>
<th>Segment</th>
<th>OBX-2</th>
<th>OBX-3</th>
<th>OBX-5</th>
<th>OBX-11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>ST</td>
<td>ETAREQ^AUSETA</td>
<td>Request with each name value pair as a repeat (replace #13#10 with ~)</td>
<td>F</td>
</tr>
<tr>
<td>Signature</td>
<td>ST</td>
<td>ETASIG^AUSETA</td>
<td>Base64 Encoded Signature, with each line as a repeat</td>
<td>F</td>
</tr>
<tr>
<td>Metadata</td>
<td>ST</td>
<td>ETAMETA^AUSETA</td>
<td>Meta with each name value pair as a repeat (replace #13#10 with ~)</td>
<td>F</td>
</tr>
</tbody>
</table>

An example message would be:

```
MSH|^~\&|PMSX21|GX3261|QMLPTX|QML^2184^AUSNATA|200004120817||
ORM^O01^ORM_O01|
GX3261_20000412-2.211|P|2.3.1|2173||AL||AU
PID|1||P00057804|PN~4099887514|MC~SMIAL001|SR||SMITH^Alan\n|Ross^Mr||
19770621|M||818 Beach Road^BEECHMERE|4510^AU|||4097859602
PV1|1||045678AB^HANDY^JOHN^Dr045678AB^HANDY^JOHN^Dr
ORC|NW|173-0^GX3261|173^GX3261|IP||200004120817||045678AB
OBR|1|^173-0^GX3261|^VAN^VANCYYCIN(PRE/POST),S^NATA2184-2||
045678AB^HANDY^JOHN^Dr|045678AB|045678AB
OBX|1|ST|ETAREQ^AUSETA|Provider: 045678AB; Dr John Handy~Pathology: Acme Pathology~Patient ID: SURG P00057804, MA 4099887514~Patient Name: ALAN R SMITH~Patient DOB: 21 Jun 1977~Request Date: 12 April 2000 08:08:33~Requests: VAN, GAM, FBC, HAB|||
OBX|2|ST|ETASIG^AUSETA|VdOYnrtjoi7LcoZnWe7NDUW4mGtOpyk+MRTsX6XR
j0gUVTBbMYQQbcRQ5sx~VASHXiKjGWhU7nW5wh1vHXw==|||
```
OBX|3|ST|ETAMETA^^AUSETA||System: Acme Inc; GP system V1.02.003
(Cust 1002)~Institution: SURG; Request Codes: AUS|||F

ORC|NW|173-1^GX3261||173^GX3261|IP|||200004120817|||045678ABOBR|2|
173-1^GX3261||GAM^IMMUNOGLOBULINS, SERUM^NATA2184-2|||||L|L|||
045678AB^HANDY^JOHN^Dr|||||^200004120817^R

ORC|NW|173-2^GX3261||173^GX3261|IP|||200004120817|||045678AB
OBR|3|173-2^GX3261||FBC^FULL BLOOD EXAMINATION^NATA2184-4|||L|L|||
045678AB^HANDY^JOHN^Dr|||^200004120817^R|0321654B^R

ORC|NW|173-3^GX3261||173^GX3261|IP|||200004120817|||045678AB
OBR|4|173-3^GX3261||HAB^HEPATITIS A \T\ B ACUTE^NATA2184-1|||L|L|||
045678AB^HANDY^JOHN^Dr|||^200004120817^R

Issues with Option #3:
(a) Structural issues with where the OBX segments are located.
(b) Choice of coding elements for OBX-3.

4.1.3.4 Option #4: new segment

In option #4, a new segment is introduced specifically to attach the digital signature to the message. This new segment bears the name ‘ZDS’ for the moment, but would be presented to the relevant HL7 committees (O/O, S&A) for consideration when fully clarified. The ZDS segment would be appended to the foot of the message.

A proposed definition for the ZDS segment:

The ZDS segment carries information about a Digital signature.

TABLE 7

<table>
<thead>
<tr>
<th>SEQ</th>
<th>LEN</th>
<th>DT</th>
<th>OPT</th>
<th>RP/#</th>
<th>TBL#</th>
<th>ITEM#</th>
<th>ELEMENT NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>250</td>
<td>CE</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>Digital Signature Type</td>
</tr>
<tr>
<td>2</td>
<td>250</td>
<td>CE</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td>Digital Signature Scope</td>
</tr>
<tr>
<td>3</td>
<td>250</td>
<td>CE</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td>Digital Signature Method</td>
</tr>
<tr>
<td>4</td>
<td>65536</td>
<td>ED</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td>Digital Signature</td>
</tr>
<tr>
<td>5</td>
<td>65536</td>
<td>ED</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td>Signing Identity</td>
</tr>
<tr>
<td>6</td>
<td>285</td>
<td>RP</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td>CA Location</td>
</tr>
<tr>
<td>7</td>
<td>65536</td>
<td>ED</td>
<td>O</td>
<td>Y</td>
<td></td>
<td></td>
<td>Attachments</td>
</tr>
</tbody>
</table>

ZDS field definitions

ZDS-1 Digital Signature Type (CE)

Definition: This field identifies the type of digital signature. This is expected to be a reference to a published standard or specification that should explain:
(a) How the digital signature is generated.
(b) How it relates to the rest of the message.
(c) How each of the fields in the rest of the segment are used.

Hereafter the specification/standard is referred to as the ‘Digital Signature Specification’.

**ZDS-2 Digital Signature Scope (CE)**

Definition: This field defines the scope of the digital signature in terms of which information in the message is covered by the digital signature. This field should only be used if the Digital Signature Specification requires it’s use. In this case, the Digital Signature Specification will define the way that the field is used.

**ZDS-3 Digital Signature Method (CE)**

Definition: This field defines the method used to generate the digital signature. Usually this would describe a PKI framework. This field should only be used if the Digital Signature Specification requires its use. In this case, the Digital Signature Specification will define the way that the field is used.

**ZDS-4 Digital Signature (ED)**

Definition: This field contains the actual digital signature. This field would generally be populated. The Digital Signature Specification will define the way that the field is used.

**ZDS-5 Signing Identity (ED)**

Definition: Information pertinent to identifying the certificate used to generate the digital signature.

**ZDS-6 CA Location (RP)**

Definition: Assist in locating the Certificate Authority for the certificate in ZDS-5.

**ZDS-7 Attachments (ED)**

Definition: Attachments as defined in the Digital Signature Specification.

Using such a signature, this specification would assign the following uses to fields of the ZDS field:

<table>
<thead>
<tr>
<th>ZDS-1 Digital Signature Type</th>
<th>Reference to this specification: ETA^^AUSSTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZDS-2 Digital Signature Scope</td>
<td>Not Used</td>
</tr>
<tr>
<td>ZDS-3 Digital Signature Method</td>
<td>Not Used</td>
</tr>
<tr>
<td>ZDS-4 Digital Signature</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>ZDS-5 Signing Identity</td>
<td>Not Used</td>
</tr>
<tr>
<td>ZDS-6 CA Location</td>
<td>Not Used</td>
</tr>
<tr>
<td>ZDS-7 Attachments</td>
<td>Attachment text/request – request document (Base64 encoded)</td>
</tr>
<tr>
<td></td>
<td>Attachment text/metadata – request metadata (Base64 encoded)</td>
</tr>
</tbody>
</table>

With this specification, the message would look like this:

```
MSH|^~\&|PMSX21|GX3261|QMLPTX|QML^2184^AUSNATA|200004120817||
ORM^O01^ORM_O01|
GX3261_20000412-2.211|P|2.3.1|2173||AL||AU
```
4.1.3.5 Verification of the Signable Document after messaging

The ETA requires that the Document’s authenticity be verifiable by the receiving system. Once the message has been decoded, the receiver must be able to verify the signature.

The receiver may also verify that the document details detailed in the Signable Document match those contained in the message. However this may not always be the case. There are several reasons why the details in the message may differ from those in the Signable Document:

(a) The Signable Document is frozen in time – Patient or provider details may have been altered between the time the request was signed and the message was generated.

(b) The request may be encapsulated in a pathology referral message where the patient and provider details are recorded differently or differently attributed.

(c) Only some of the items requested in the test may be requested in the message (particularly for referrals).

(d) The items requested may have been translated to a different code set.

Receiving systems should not automatically expect the contents of the Signable Request contained in a message to correspond to those of the message. Implementers will need to decide what level of verification is performed by the receiving system.
APPENDIX A

Informative / Normative

A1 TestPatient.oru

MSH|^~\&|TEST^TESTAPP^L|Buderim GE Centre|^7C3E3681-91F6-11D2-8F2C-444553540000^GUID|||20040410141133||ORU^R01|20040410.1061990||2.3.1^0.9^AU S|||AL||AU

PID|1|||PATIENT^Test^^^^^^L||20000101|||139 King Street|^BU DERIM^QLD^4556^AU^C|AU

PV1|1|O|0341615J^WHITE^MELISSA^^^DR^^^AUSHICPR^L^UPIN||0341615J^ WHITE^MELISSA^^^DR^^^AUSHICPR^L^UPIN|||N

ORC|CE|^F71DEE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre|^7C3E3681-91F6-11D2-8F2C-444553540000^GUID|||28655-9^Physician Discharge Summary^LN|||20040410141133|||0341615J^WHITE^MELISSA^^^DR^^^AUSHICPR^L^UPIN|||LN&F71DEE61-D19E-4571-AF7B- BF8C74597CAB||20040410140303||PHY|F|20040410|0341615J^WHITE^MELISS A^^^DR^^^AUSHICPR^L^UPIN||0191322W&MCINTYRE&ANDREW&&&Dr& MBBS FRACP&AUSHICPR&&L&||&UPIN

OBX|1|FT|28655-9^LN||This a simple Test Message To demonstrate signing and another Line A few encoded characters

A2 TestPatientETA.oru

MSH|^~\&|TEST^TESTAPP^L|Buderim GE Centre|^7C3E3681-91F6-11D2-8F2C-444553540000^GUID|||20040410141133||ORU^R01|20040410.1061990||2.3.1^0.9^AU S|||AL||AU

PID|1|||PATIENT^Test^^^^^^L||20000101|||139 King Street|^BU DERIM^QLD^4556^AU^C|AU

PV1|1|O|0341615J^WHITE^MELISSA^^^DR^^^AUSHICPR^L^UPIN||0341615J^ WHITE^MELISSA^^^DR^^^AUSHICPR^L^UPIN|||N

ORC|CE|^F71DEE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre|^7C3E3681-91F6-11D2-8F2C-444553540000^GUID|||28655-9^Physician Discharge Summary^LN|||20040410141133|||0341615J^WHITE^MELISSA^^^DR^^^AUSHICPR^L^UPIN|||LN&F71DEE61-D19E-4571-AF7B- BF8C74597CAB||20040410140303||PHY|F|20040410|0341615J^WHITE^MELISS A^^^DR^^^AUSHICPR^L^UPIN||0191322W&MCINTYRE&ANDREW&&&Dr& MBBS FRACP&AUSHICPR&&L&||&UPIN

OBX|1|FT|28655-9^LN||This a simple Test Message To demonstrate signing and another Line A few encoded characters
A3 TestPatientMD5.oru

MSH|^~\&|TEST^TESTAPP^L|Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||20040410141133||ORU^R01|20040410.1061990||2.3.1^0.9^AU\S|||AL|AU

PID|||PATIENT^Test^^^^^^L||20000101||139 King

Street^BUDERIM^QLD^45666^AU|CAU

PV1[1][0]|0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN|0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN|||N

ORC|CE||F71DE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||CM||||||0341615J^WHITE^MELISSA^DR^AUSHICPR^L^UPIN^UPIN

OBR|1|F71DE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID|28655-9^Physician Discharge

Summary^LN||20040410||||0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN|||LN&F71DE61-D19E-4571-AF7B-BF8C74597CAB^20040410140303|PHY|F|0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN||0191322W&MCINTYRE&ANDREW&Dr&MBS FRACP&AUSHICPR&L&UPIN

OBX|1|FT|28655-9^LN||This a simple \H\Test Message\N\ To demonstrate signing and \H\ORU\N\ message.\br\\br|Another Line \br\br|A few encoded characters

\FS\NF\TV|\br|\br|The end|||F

OBX|1|SN|5048-4^ANA titre^LN|<40itre|||F

OBX|2|FT|SIGNATURE_HEADER^^L||Patient: PATIENT, Test


OBX|3|ST|AUSMD5HASH^Message Digest^L||3db58fc969685ca54c73620d3ee3e98c|||F

A4 TestPatientSHA1.oru

MSH|^~\&|TEST^TESTAPP^L|Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||20040410141133||ORU^R01|20040410.1061990||2.3.1^0.9^AU\S|||AL|AU

PID|||PATIENT^Test^^^^^^L||20000101||139 King

Street^BUDERIM^QLD^45666^AU|CAU

PV1[1][0]|0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN|0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN|||N

ORC|CE||F71DE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID||CM||||||0341615J^WHITE^MELISSA^DR^AUSHICPR^L^UPIN^UPIN

OBR|1|F71DE61-D19E-4571-AF7B-BF8C74597CAB^Buderim GE Centre^7C3E3681-91F6-11D2-8F2C-444553540000^GUID|28655-9^Physician Discharge

Summary^LN||20040410||||0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN|||LN&F71DE61-D19E-4571-AF7B-BF8C74597CAB^20040410140303|PHY|F|0341615J^WHITE^MELISSA^DR^AUSHICPR^L^^UPIN||0191322W&MCINTYRE&ANDREW&Dr&MBS FRACP&AUSHICPR&L&UPIN

OBX|1|FT|28655-9^LN||This a simple \H\Test Message\N\ To demonstrate signing and \H\ORU\N\ message.\br\\br|Another Line \br\br|A few encoded characters

\FS\NF\TV|\br|\br|The end|||F

OBX|1|SN|5048-4^ANA titre^LN|<40itre|||F

OBX|2|FT|SIGNATURE_HEADER^^L||Patient: PATIENT, Test


OBX|3|ST|AUSMD5HASH^Message Digest^L||3db58fc969685ca54c73620d3ee3e98c|||F
Discharge Summary

This is a simple Test Message To demonstrate signing and another Line A few encoded characters

Patient: PATIENT, Test
DOB: 01.01.2000
Report: Physician Discharge Summary Dated: 10.4.2004
Signed: 10/04/2004 2:28:49 PM

Message Digest
3NziMKlseL7b9H6+uKsj9ZBM2M=