Contents

Status of this Guide .......................................................................................................................... 4

Introduction ...................................................................................................................................... 4
  Overview ........................................................................................................................................ 4
  Assumptions .................................................................................................................................. 4
  Requirements ................................................................................................................................. 4

1.0 The X-Direct-Context Header .................................................................................................... 5

2.0 Metadata: MIME Headers and Encoding ..................................................................................... 5

3.0 Metadata: Content ....................................................................................................................... 5
  3.1 Version ...................................................................................................................................... 6
  3.2 Transaction ID ........................................................................................................................... 6
  3.3 Patient ID .................................................................................................................................. 7
  3.4 Transaction Type ....................................................................................................................... 7
  3.5 Purpose of Use ........................................................................................................................... 8
  3.6 Patient Matching Parameters ..................................................................................................... 8
  3.7 Encapsulation of Other Data Types ........................................................................................... 9

4.0 Recipient Responses: Error Conditions ...................................................................................... 10
  4.1 Version Not Supported .............................................................................................................. 10
  4.2 Transaction Type Not Supported ............................................................................................... 10

5.0 Security Considerations ............................................................................................................. 10

6.0 Acknowledgements ................................................................................................................... 10

7.0 References .................................................................................................................................. 11
## Change Control

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>06-20-2016</td>
<td>0.1</td>
<td>Initial Draft</td>
</tr>
<tr>
<td>10-18-2016</td>
<td>1.0-DRAFT-2016101801</td>
<td>Addresses feedback from Direct Project Implementers Workgroup.</td>
</tr>
<tr>
<td>12-29-2016</td>
<td>1.0-DRAFT-2016122901, Draft for Trial Use</td>
<td>Incorporates final set of feedback from Direct Project Implementers Workgroup (IWG) gathered in October 2016 meeting. Per IWG, this draft is offered for trial use and additional feedback prior to further advancement.</td>
</tr>
</tbody>
</table>
Status of this Guide

This document is DRAFT and is offered FOR TRIAL USE.

Introduction

Overview

This document defines an extensible mechanism to express the context of a Direct message exchange by providing a framework for the inclusion of contextual metadata by the message sender. Such metadata may be helpful for routing and processing of Direct messages, such as in cases where the payload format contains limited or no intrinsic metadata, or when the reason for the transmission may not be easily determined from the payload content.

The framework was designed so that the metadata could also be available to users of non-conforming applications in a human-readable format. A separate attachment containing the payload metadata was selected over a series of RFC 822 headers, as such headers may not be as easily viewed by all Mail User Agents (MUAs). Similarly, human-readable metadata parameters and values were selected over Object Identifiers (OIDs) or other non-human-readable representations.

Assumptions

It is assumed that any Direct message (including any mail system reports such as Delivery Status Notifications), header, or attachment described in this document conforms to the requirements of Direct Project's Applicability Statement for Secure Health Transport v1.2, referred to as "Applicability Statement" in subsequent sections.

Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

An implementation is not compliant if it fails to satisfy one or more of the MUST, SHALL, or REQUIRED level requirements for the protocols it implements. An implementation that satisfies all the MUST, SHALL, or REQUIRED level and all the SHOULD level requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the MUST, SHALL, or REQUIRED level requirements but not all the SHOULD level requirements for its protocols is said to be "conditionally compliant."
In addition, annotations called “Implementation Note:” are used to provide additional clarification to implementers. These are non-normative and provided for clarification and informational purposes only.

1.0 The X-Direct-Context Header

A sending system SHALL indicate its conformance to this guide by including the following header with the RFC 822 headers of the Health Content Container (as defined by the Applicability Statement):

```
X-Direct-Context: <cid-identifier>
```

The MIME body of the conforming Health Content Container SHALL be a MIME multipart container. The cid-identifier in the X-Direct-Context header SHALL correspond to the value of a Content-ID header of the MIME part that contains the Metadata attachment (see Section 2.0 of this document), as per RFC 2045. The MIME part referenced by the Content-ID header SHALL NOT be nested within another MIME multipart container. Only a single context is permitted per message. When multiple attachments are included by a sender, the same context SHALL apply to all attachments.

2.0 Metadata: MIME Headers and Encoding

A sending system SHALL include an attachment within a conforming Direct message that contains the payload metadata. This MIME part shall be identified by a Content-ID header field with a value equal to the cid-identifier specified in the X-Direct-Context header as defined in Section 1.0 of this document.

In order to permit implementations that do not conform to this guide to provide the metadata in a human readable form to operators, the MIME part MUST contain the following headers:

```
Content-Type: text/plain
Content-ID: <cid-identifier>
Content-Disposition: attachment; filename=metadata.txt
```

Line breaks in this attachment must by canonicalized to <CR><LF> in accordance with the relevant RFCs. If the attachment contains any 8-bit-wide words (such as with the use of certain UTF-8 characters), an appropriate content encoding MUST be applied.

3.0 Metadata: Content

The content of the metadata attachment SHALL be structured as a series of one or more metadata elements expressed as parameter/value pairs, separated by line breaks, as defined
further in the following subsections. Lines that begin with whitespace shall be treated as
continuations of the preceding line. The ABNF notation used in this guide conforms to RFC 5234.

\[
\text{metadata} = 1^* (\text{metadata-element} \ CRLF) \\
\text{metadata-element} = \text{metadata-parameter} \ "\" \text{metadata-value} \\
\text{metadata-parameter} = <\text{printable ASCII characters other than whitespace} \text{ and } \"\"> \\
\text{metadata-value} = <\text{printable ASCII characters with additional restrictions as appropriate for each header; leading or trailing whitespace is ignored}>
\]

Each metadata parameter MAY specify additional requirements for allowed metadata values, and
MAY specify cardinality requirements on the parameter itself. Metadata parameter names are
case-insensitive. Metadata values are case-insensitive, unless specified otherwise in this guide. All
metadata-elements listed below are OPTIONAL, unless otherwise specified.

A conforming system MUST understand the version-element, and MUST conform to any
requirements below where metadata must be echoed in response messages. Otherwise, a
receiving system MAY use the enclosed metadata in any manner it chooses, including ignoring
the metadata or subsets of the metadata.

### 3.1 Version

\[
\text{version-element} = \text{"version:"} \ \text{version-identifier} \\
\text{version-identifier} = \text{"1.0"}
\]

The metadata MUST include one version-element. Future versions of this document that
introduce new functionality that is not backwards compatible with this version SHALL increase
the numeric value of the version-identifier.

### 3.2 Transaction ID

\[
\text{id-element} = \text{"id:"} \ \text{unique-identifier}
\]

The id-element defines a unique and persistent identifier assigned by the originating party to
uniquely identify a sequence of related transactions, such as a query and response or an order for
a diagnostic test and its result. This id-element also correlates any error reporting or required
acknowledgments when this is not already encapsulated in the message content. The unique-
identifier MAY be the same as the Message-ID of the message if appropriate. Only one
id-element is permitted in the metadata. When responding to a message that contains this
element, the same id-element SHALL be included in the response metadata.

Examples:

- id: <2142848@direct.example.com>
- id: 2ba8a9a1-0f59-4688-b818-67930ae26979
3.3 Patient ID

patient-id-element = “patient-id:” pid-instance *(“;” pid-instance)
pid-instance = pid-context “:” local-patient-id
pid-context = <Assigning Authority Domain ID or UUID as described in text below>
local-patient-id = <printable ASCII characters other than whitespace and “;”>

The sender of a Direct message who wishes to identify the patient identifier in its local context SHALL construct a pid-instance using its unique Assigning Authority OID and its local patient identifier. The pid-context value is a globally unique value for each issuer of patient identifiers. If the sender has an Assigning Authority Domain ID (AA) that it uses for transactions under the Integrating the Healthcare Enterprise Information Technology Infrastructure Technical Framework (IHE ITI TF), then the sender SHOULD use that ID as the pid-context. If such an AA is not used, then the sender MUST use a Name-Based Universally Unique Identifier (UUID) as defined in Section 4.3 of RFC 4122 using the sender’s Direct Address or Direct Domain as the input, with the resulting 16 octet UUID value expressed as an unsigned integer as the final value of an OID in the 2.25 OID arc (e.g., a UUID with an unsigned integer value of 123456789 would be expressed as 2.25.123456789). At most one patient-id-element is permitted in the metadata. All pid-instances are intended to represent the same patient in the corresponding pid-context, thus each context may correspond to at most one patient. Only one pid-instance is permitted per pid-context, i.e. a pid-context MUST NOT appear more than once in a single patient-id-element. A party MAY add, modify, or remove its own pid-instance when constructing the patient-id-element in responses. Otherwise, each pid-instance included in an incoming message MUST be included in the response. Each participant SHOULD include its preferred patient identifier as its local-patient-id.

Example:

patient-id: 2.16.840.1.113883.19.999999:123456;
2.16.840.1.113883.19.888888:75774

3.4 Transaction Type

type-element = “type:” category “/” action
category = “laboratory”
/ “radiology”
/ “pharmacy”
/ “referral”
/ “general”
action = “order”
/ “report”
/ “result”
/ “query”
When a type-element is included in the metadata, the action is intended to identify the role of the message sender in the transaction sequence, i.e., a query action would generally be followed by a response action.

Example:

```
type: radiology/report
```

*Implementation Note:* For the purpose of trial use of the type-element, the above vocabulary for category and action values is intended to be normative, i.e., other values are not permitted. It is expected that additional useful category and/or action values will be identified by the Direct community during the trial use of this guide and that proposed modifications to the above value sets will be evaluated during the next update to this document.

### 3.5 Purpose of Use

```
purpose-element = "purpose:" purpose-name
purpose-name = "treatment" / "payment" / "operations" / "emergency" / "research"
```

When a message sender requests the disclosure of healthcare information from the recipient, the purpose-element identifies the purpose for which the sender will use the disclosed information.

### 3.6 Patient Matching Parameters

```
patient-data-element = "patient:" patient-attribute *(";"
patient-attribute) = patient-parameter "=" patient-parameter-value
patient-parameter = "givenName"
/ "surname"
/ "middleName"
/ "dateOfBirth"
/ "gender"
/ "socialSecurityNumber"
/ "telephoneNumber"
/ "streetAddress"
/ "postalCode"
patient-parameter-value = <based on patient-parameter, see text below for additional details and restrictions>
```

Both the patient-parameter and patient-parameter-value are case insensitive. The patient-parameter-value format is defined based on the patient-parameter and MUST NOT contain the ";", CR, or LF characters. Contiguous whitespace MUST be treated as a single space. Leading and trailing whitespace MUST be ignored. A patient-parameter
MUST NOT appear more than once in the patient-data-element. When a parameter is included, the following additional requirements apply:

- **dateOfBirth**: MUST be in YYYY-MM-DD or YYYY format (if month/day are unknown)
- **socialSecurityNumber**: MUST contain 9 digits or last 4 digits; MAY include hyphens
- **telephoneNumber**: MUST contain 10 digits, including area code; MAY include parentheses or hyphens
- **postalCode**: MUST contain 5 digit or 9 digit zip code; MAY include a hyphen
- **middleName**: MUST contain middle name or first letter of middle name; MAY include first letter plus a period.

Example:

```
patient: givenName=John; surname=Doe; dateOfBirth=1961-12-31
```

This metadata is included to facilitate patient matching by the recipient when the recipient’s patient identifier is not known to the sender. The recipient MAY disregard any characters in the parameter values that are classified under the “MAY” clauses above, e.g., parentheses in a telephone number. If a patient-id-element is included for the recipient’s domain, the recipient SHOULD disregard the patient-data-element.

### 3.7 Encapsulation of Other Data Types

```
encapsulation-element = “encapsulation:” encapsulated-message-type
encapsulated-message-type = “http” / “hl7v2”
```

This metadata element MUST be included when Direct is used as a transport to encapsulate other message types such as an HTTP request or response, or HL7 v2 message or acknowledgement.

The `encapsulated-message-type"http"` MUST be used for encapsulated HTTP RESTful transactions such as with HL7 Fast Healthcare Interoperability Resources (FHIR) or encapsulated HTTP SOAP transactions such as transactions defined by the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework. The `encapsulated-message-type"hl7v2"` MUST be used for encapsulated HL7 V2 transactions.

To encapsulate an HTTP transaction or its response, the HTTP headers and, if applicable, any POST data or other content SHALL be included in one or more separate attachments with the MIME type of `application/x-direct-encapsulated+http`. To encapsulate an HL7 V2 message or its response, the HL7 V2 message data SHALL be included in one or more separate attachments with MIME type of `application/x-direct-encapsulated+hl7v2`. Encapsulated HL7 V2 messages SHALL NOT include any control codes required by the HL7 V2 low level protocol (LLP).

When more than one encapsulated message is included by the sender, the recipient MUST process the attachments in the order that the corresponding MIME attachments were included.
by the sender. A recipient MUST process each encapsulated message even if an earlier message
results in an error, and MUST include the encapsulated responses in the same order in the
response message. Thus, the sender MUST NOT assemble a sequence of attachments where the
message encapsulated in one attachment depends upon or assumes the successful processing of
an earlier attachment in the sequence. If the assembled responses would exceed a sender’s
outgoing message size limits, the sender MAY send a failure message instead.

This guide does not provide a mechanism to insert the results of one encapsulated transaction
into the next encapsulated transaction when multiple transactions are included in a single
message.

4.0 Recipient Responses: Error Conditions

4.1 Version Not Supported

A conforming system MAY reject a message when the metadata version-identifier
specified by the sender is not supported by returning a Delivery Status Notification (DSN) with
action-value of failed and status-code of "5.3.3" (indicating "System not capable of
selected features").

4.2 Transaction Type Not Supported

A conforming system MAY reject a message when the transaction type specified by the sender is
not supported by the receiving endpoint by returning a Delivery Status Notification (DSN) with
action-value of failed and status-code of "5.3.3" (indicating "System not capable of
selected features"). For example, an immunization registry endpoint MAY reject a message when
the context includes a type-element of “type: radiology/order”.

5.0 Security Considerations

In addition to the security considerations described in the Applicability Statement, implementers
should consider security and privacy issues related to patient matching accuracy based on the
available metadata.

6.0 Acknowledgements

This document was written by the Direct Project Implementers Workgroup.

Editors: Luis Maas and John Hall
7.0 References

1. Applicability Statement for Secure Health Transport v1.2
2. RFC 822 - Standard for the Format of ARPA Internet Text Messages
3. RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
4. RFC 2119 - Keywords to use in RFC’s for Requirement Levels
5. RFC 4122 - A Universally Unique IDentifier (UUID) URN Namespace
6. RFC 5234 - Augmented BNF for Syntax Specifications: ABNF