A Report on DirectTrust Interoperability Testing and Recommendations to Improve Direct Exchange

TECHNICAL WHITE PAPER

Authors: Julie Maas, CEO, EMR Direct; David C. Kibbe, President and CEO, DirectTrust; and the DirectTrust Security and Trust Compliance Workgroup

Draft for Public Comment, March 18, 2015
# Table of Contents

Executive Summary .................................................................................................................................................. 3
1 Introduction ......................................................................................................................................................... 6
2 Interoperability Challenges and Solutions: Content/Payload and Edge Systems ........................................... 10
3 Interoperability Challenges and Solutions: Health Information Service Providers (HISPs) and Security/Trust Agents (STAs) ........................................................................................................... 16
4 Interoperability Challenges and Solutions: Certification Authorities ................................................................. 20
5 Interoperability Challenges and Solutions: On the Wire, Between HISPs ......................................................... 22
6 Interoperability Challenges and Solutions: Management Issues .......................................................................... 22
7 Recommended Changes to Existing Specifications ............................................................................................ 25
8 Recommended Best Practices for the Next Phase of Direct Exchange ............................................................... 27
9 Conclusions ....................................................................................................................................................... 28
EXECUTIVE SUMMARY

Direct exchange is a robust, inexpensive solution that uses mature Internet data transport and encryption technologies to provide healthcare interoperability. Direct was designed to offer a secure way for electronic health record (EHR) users to “push” messages containing sensitive protected health information (PHI) to other EHR users, across the boundaries of organizations and IT systems. “Interoperability” results from Direct when a user of an EHR system is successful in exchanging PHI with users of other EHR systems without special effort.

As a result of work accomplished during the last two years, sufficient infrastructure exists today to support widespread use of Direct messaging within the U.S. health care system. Direct is a federal standard that is required of EHR technologies as part of the certification¹ program operated by the Office of the National Coordinator for Health IT (ONC), and DirectTrust has established a network of Direct service providers (also known as Health Information Service Providers or HISPs) that currently enables Direct exchange at over 35,000 health care organizations in which over 660,000 professionals have Direct addresses and are capable of sending and receiving Direct messages from within their EHRs. Significant continued growth of this network is expected during 2015 and 2016.

However, as this Report describes in detail, the introduction of any new and complex technology such as Direct exchange involves numerous challenges and requires problem solving and mid-course corrections before its use is deemed highly reliable and the user experience is consistently a good one. In the particular case of Direct, optionality in the Direct specifications² and certification criteria permits design choices by HISPs and EHRs implementing Direct in the field that may not be focused on seamless, robust interoperability. The most significant category of unresolved issues arises from the payload (the attachment accompanying the message) not being sufficiently constrained, resulting in data sets that can be understood by one system, but not by every other. Also, Direct certification testing does not require that every system under test demonstrate the ability to process both of the acceptable content message container types, either of which may be transmitted as Direct payloads for attestation purposes under the Meaningful Use programs. This variability can mean a sub-par customer experience to providers using certain EHR technologies even when the transport for exchange is successful.

¹ Certification testing or simply certification as used in this Report refers to certification of an EHR technology under the Office of the National Coordinator for Health Information Technology’s 2014-2015 Edition Electronic Health Record (EHR) Certification Criteria and Standards Rule.

² The Direct specifications are defined by multiple documents, each covering a different aspect of Direct exchange. These include the Applicability Statement for Secure Health Transport, the Implementation Guides for Certificate Discovery, Delivery Notification, Trust Bundle Distribution, Edge Protocols, and the XDR and XDM for Direct Messaging Specification. The following RFCs are also closely related to the above documents, and an understanding of these additional documents by Direct service providers is also required: RFC 2315, 2585, 2782, 2821, 3798, 4398, 4511, 4516, 5280, 5322, 5652, 5751, 5752. Collectively, these documents form what is referred to in this paper as the Direct specification, the Direct protocol, or simply specification or protocol, unless specifically noted otherwise.
Further, when the requirements of the Direct standard are not well-executed by all service providers and every EHR endpoint, the result may be a provider’s inability to deliver optimal patient care.

Extensive “in the field” testing of many thousands of Direct exchanges by DirectTrust member HISPs has brought this community to the point where we are able to summarize what we have learned to date and can be specific in recommending best practices for Direct implementers that will make interoperability using Direct more seamless and reliable. We believe acceptance of these best practices will bring us one step closer to the improved user experience healthcare providers and citizens are expecting from their EHR technology investments. This Report organizes “Interoperability Challenges and Solutions” into several categories; explains the problems that have been discovered by DirectTrust members over time; discusses these in detail; and, where possible, offers practical solutions that we hope will be carefully addressed by each of the participants in Direct exchange, including all HISPs and all EHR vendors, and in the spirit of collaboration and cooperation that has characterized this work to date.

However, the private sector alone cannot solve all of the problems that have been encountered, nor make all of the improvements that are suggested in this Report. Governmental action in collaboration with the private sector is required if we are going to make rapid and near term progress in achieving interoperability among EHRs using Direct, and reach the goal of interoperability for Stage 2 Meaningful Use that was first articulated when the Direct Project was started in 2011. We especially call upon ONC, CMS, and HHS to work with the private sector, including HISPs, EHRs, and, very importantly, the health care professionals and hospitals who are engaged in meeting the objectives and metrics of Stage 2 Meaningful Use, to bring Direct exchange to maturity and ubiquitous use by the end of 2015.

This Report will provide background information and discussion in support of the following specific and actionable recommendations:

RECOMMENDATION 1. We encourage the Office of the National Coordinator for Health IT (ONC) at the earliest possible date to convene an appropriate forum and designate a process to revise and make improvements to the Applicability Statement for Secure Health Transport and other specification documents for Direct exchange, including specifications for payload types required for certification, with the purpose of removing ambiguity, clarifying inconsistent uses of component standards, providing guidance to improve compatibility between the endpoint applications that both send and receive Direct messages, and with attention to those elements pertinent to the use of Direct to attest to Meaningful Use.

Of particular importance are changes and guidance that would remove ambiguity by narrowing the list of acceptable variations in what constitutes a valid Direct payload under the Consolidated Clinical Document Architecture (C-CDA, an XML data structure consisting of HTML-like tags around data elements); publication of a specification for converting from XDM Zip to MIME payloads as well as enumeration of who is required to implement the specification; setting expectations

---

3 When C-CDA is mentioned in this report, it is referring specifically to a C-CDA payload that is compliant with the Office of the National Coordinator for Health Information Technology’s 2014 Edition Criteria and Standards Rule.

4 XDM Zip and MIME are two different payload content formats permitted for attestation in use of the Direct specifications for transitions of care as part of Stage 2 of Meaningful Use.
regarding a number of service level issues that manifest themselves when sub-systems are inadequately monitored by the Direct service provider; and clarifying the use of Message Disposition Notifications, MDNs, which notify the sender of a Direct message that the receiving entity has been reached. Details regarding the challenges posed to Direct exchange interoperability and observations revealed during DirectTrust interoperability testing will be discussed in detail in the body of the Report.

RECOMMENDATION 2. We recommend the establishment of an additional and focused layer of certification that will test the “real world” capabilities of EHR technologies to send and receive Direct messages; demonstrate the usability of EHR technologies for this purpose; and capture and bring more openly into the public domain those limitations and barriers to interoperability noted in this Report, as well as others that may be discovered in the future. We encourage ONC, possibly in concert with other responsible entities within the Department of Health and Human Services (HHS), or the Food and Drug Administration (FDA), and working with the private sector, health information exchange governance entities, EHR certifying bodies, and other federal agencies involved in the use of Direct exchange, to pursue such certification within the next twelve months.

Though many different issues are discussed in this Report, we should be clear about one thing: there is simply no excuse for lack of interoperability in health care. There are plenty of reasons why implementing cryptographic software is challenging, but there are no policy, technical, or cost barriers that should prevent successful, large-scale adoption and interoperability via Direct. A Direct connection to a HISP is reusable and scalable, and a more cost-effective healthcare interoperability architecture is not known at this time. Further, any similar technology focused on healthcare interoperability would be faced with most if not all of the same last-mile challenges. Any single issue that might arise with Direct is certainly addressable on its own in the field today, however network-wide solutions are known to be more effective in solving interoperability issues at scale.
1 INTRODUCTION

DirectTrust is a non-profit trade alliance that supports health information exchange among providers, provider organizations, and patients/consumers using the Direct specifications for secure, interoperable, and identity validated messages. Direct exchange combines mature Internet data transport and encryption into a vendor-neutral protocol for electronic health record (EHR) users to “push” messages containing sensitive protected health information (PHI) to other EHR users, across the boundaries of organizations and IT systems (see Figure 1). Efficiency is gained by leveraging protected health information resources at the “edges” of the network, without the need for a central data handler or controller. Trust among relying parties in such exchanges is made scalable through DirectTrust’s security and trust policy framework, which is the basis of an accreditation and audit program that DirectTrust offers in partnership with the Electronic Health Network Accreditation Commission (EHNAC) and through the operation of DirectTrust’s network services that include DirectTrust trust anchor bundles. These offer accredited Direct exchange service providers (HISPs) a convenient way to assert and maintain trusted relationships across their networks consisting of providers and provider organizations using Direct exchange, and without requiring one-to-one negotiations or contracts, which would be prohibitively expensive. As of the end of 2014, 38 DirectTrust in-bundle HISPs were providing a “network of networks” that included over 300 electronic health record systems (EHRs) and 50 Health Information Exchanges (HIEs), linking over 35,000 health care organizations (HCOs) and over 660,000 individual Direct exchange end users with Direct addresses.

From March, 2013 to March, 2015, the work of DirectTrust to establish its governance structure, security and trust policies, accreditation programs, and trust anchor bundle network services has been supported through a grant associated with the award of a Cooperative Agreement as part of the Exemplar Health Information Exchange Governance Program from the Office of the National Coordinator for Health IT, ONC. Total grant funding awarded over the two year Cooperative Agreement was $330,205.

Interoperability means the ability of a system to exchange electronic health information with and use electronic health information from other systems without special effort on the part of the user. Testing is required in order to confirm, initially and on an ongoing basis, that different systems can interoperate by successfully exchanging Direct messages across the network. This includes the ability for endpoints to consume the payloads (attachments) they receive. Achieving interoperability is no small task, but DirectTrust benefits from the robust spirit of collaboration within its membership, in which competitors


6 See The Office of the National Coordinator for Health Information Technology publication Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, DRAFT Version 1.0.
have come together to share information with each other for the benefit of achieving interoperability between the products and organizations involved.

Figure 1 illustrates several key features of Direct exchange. Both the sender and receiver have Direct addresses of the type Name@Direct.HealthCareOrg.com; each is accessing Direct via an “edge client” application, usually an EHR; the Health Information Service Provider (HISP) manages the processes of encryption/decryption of messages and sending/receiving these over the Internet. Interoperability is achieved when sender and receiver are in different organizations and use different EHR products, but the messages can be understood and processed.

DirectTrust has encouraged interoperability testing since its Transitional Trust Anchor Bundle (TTAB) was first launched in August, 2013. Building upon the tradition of developer Connect-a-thons established by the Direct Project, interoperability testing continued informally between DirectTrust member HISP member HISPs until a more formal testing process was established by the Security and Trust Compliance Workgroup in February, 2014. HISP-to-HISP interoperability testing has been the main focus of this testing, with the goal of providing a robust network backbone. Evaluation and discussion of EHR-to-EHR testing and its associated challenges are also occurring and assuming more importance as HISP-to-HISP interoperability testing is becoming routinized and actual HISP-to-HISP transport has gained stability. DirectTrust has developed tools for reporting interoperability testing results by HISPs and application endpoints, e.g. EHRs, PHRs, and web applications, and the results are regularly incorporated into color-coded matrices that reflect network-wide test results in a single view.
Payloads specific to Stage 2 of Meaningful Use\(^7\) (MU2) are necessarily the first priority to evaluate where end-to-end interoperability of Direct exchange is concerned, since these are required uses of the Direct protocol for eligible providers and hospitals engaged in Meaningful Use programs. But it should be recognized that uses of Direct extend beyond those required by Meaningful Use Stage 2 (criteria 170.314(b)(1), 170.314(b)(2), and 170.314(e)(1)), since any type of digital payload that can be sent by email can be attached to a Direct message. Direct can optionally be used for Secure Messaging between patient and provider, under Meaningful Use Stage 2 criterion 170.314(e)(3). Further, Direct can be used outside the context of an EHR: any application that requires exchange of electronic Protected Health Information can leverage Direct.

As interoperability issues are reported, DirectTrust members share details about their findings within the Security and Trust Compliance Workgroup, which meets regularly every two weeks. The formal discussion of these issues within the workgroup leads to progress in consensus interpretation of standards and policies, identification of the causes of variability and the shortcomings of the existing specifications brought to light through the deployment of Direct exchange at scale, and eventual determination of best practices for improved interoperability. The solutions reached by HISPs both independently and in collaboration within the Workgroup are also fed back into DirectTrust’s policy making, and strengthen DirectTrust requirements through the addition of new accreditation criteria or refinement and clarification of existing criteria.

A recent snapshot of the DirectTrust Transitional Bundle HISP-to-HISP interoperability testing results matrix is shown in Figure 2.

---

\(^7\) The authors assume readers will have a basic familiarity with the program and stages of the Medicare and Medicaid EHR incentive payment programs, commonly referred to as Meaningful Use. For those unfamiliar, we recommend as a starting point for information the HealthIT.gov website [http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives](http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives).
Each HISP is encoded with a shade of blue. The darkest blue indicates an accredited HISP that has been accepted into the DirectTrust Accredited Trust Anchor Bundle, ATAB. The middle shade indicates an accredited HISP that has not yet been accepted into the ATAB. The lightest shade indicates a HISP that is a candidate for accreditation but has not yet been accredited.

“Success” is defined as both the receipt of a readable message as confirmed by the recipient and the receipt of the expected Message Disposition Notification (MDN) by the sender. Green squares between counter parties represent successful transmission between the sending HISP listed in the left column and the receiving HISP along the top row. The top row of recipients consists of the same HISPs from left to right that are listed along the left hand side, from top to bottom. Yellow squares represent “partial success”. Partial success may occur when the right type of MDN was not returned or the recipient did not confirm that the message was received and readable. Other examples of partial success may include certificate, encryption, or signature issues. Red squares indicate “no success”—that the sender was unable to transmit a message to the recipient because the message never left their system or an immediate failure was received. White squares appear where no results have been reported for the associated sender/recipient pairing.

Most of the issues that initially resulted in partial success have been resolved within the DirectTrust community of HISPs and CAs, and the most commonly encountered of these will be discussed in this Report.
To the right of the main sender/recipient matrix are summary interoperability scores for each HISP. The first column is a total of all the green squares for each sender, the maximum achievable result at this time being thirty. The second column is a total computed only for accredited HISPs, and reflects successful transmissions to other accredited HISPs, the maximum achievable result at this time being twenty-eight. These first two columns are color coded from red to green, with red indicating the lowest values and green indicating the highest. The third column is the percentage of accredited HISPs with whom each accredited sender is green, from 0% to 100%. A score of 100% indicates that a HISP has demonstrated full baseline interoperability with all other accredited HISPs.

The sections that follow will describe the interoperability barriers and solutions discussed as part of this testing program, and as introduced to the workgroup in the context of its responsibility for the management of accreditation compliance issues. The topics are categorized according to the technical or management areas to which they pertain. Figure 3 may assist the reader in visualizing the boundary of the DirectTrust security and trust framework, the HISP functionality within it, and the edge systems such as EHRs, patient portals, and other applications beyond the boundary of the security and trust framework.

![DirectTrust Network Diagram](image)

Figure 3 DirectTrust Network Diagram

2 **INTEROPERABILITY CHALLENGES AND SOLUTIONS: CONTENT/PAYLOAD AND EDGE SYSTEMS**

While Direct can be used to send many different payload types as part of many different use cases, this section will focus on the use case in which Direct exchange is used by providers who will attest to the objectives of Meaningful Use Stage 2 (MU2) associated with “transitions of care,” highlighting several payload issues that are currently barriers to interoperability for this common and important use case. Payload interoperability challenges impact multiple sending endpoints and multiple recipients simultaneously. Thus, their high degree of incidence should translate to great benefit from additional guidance in the form of revised specifications and the industry best practices described in this Report.
To be clear, these issues do not relate to the successful technical deployment of Direct as a transport method for data but rather to the use of Direct to transmit specific payloads for this particular use case.

In order to attest to MU2 objectives and metrics, and thus receive incentive payments from either Medicare or Medicaid, eligible providers and hospitals are required to use EHR technology that has been certified by ONC to have met specific criteria and standards. Such certification requires demonstration by an EHR technology under test that a valid C-CDA payload can be created and transmitted by an EHR system as an attachment to a Direct message, and that the system can also incorporate C-CDA data similarly received as an attachment. This is often referred to as “Vanilla Direct”, indicating it is the simplest, most basic case.

The first part of the content/payload challenge pertains to the content of the C-CDA document itself. Interoperability is often declared broken when the receiver is unable to ultimately parse and consume the content of the C-CDA, due to structural issues such as extra or missing XML elements, or other variability introduced by differences in interpretation of the C-CDA standard by the sending EHR system’s developers and the receiving EHR system’s developers. It has been suggested that a more highly-constrained C-CDA format is needed to resolve this type of issue by reducing variability of the C-CDA structures produced by different vendors.

Additionally, active testing of a system’s ability to consume C-CDAs generated by multiple vendors is expected to make this process the most efficient and productive by identifying the real world collisions that may not be evident when testing against a single common validation tool. Toward this goal, DirectTrust distributes a testing Trust Bundle that is designed to network EHR vendor test environments, to facilitate the software iteration likely needed to improve the structure of the C-CDA itself and how it is implemented in EHR applications. In addition, DirectTrust’s existing tool for reporting HISP-to-HISP interoperability testing was designed to be able to collect information on end-to-end exchanges between different pairs of EHR technologies to document and quantify the degree of end-to-end C-CDA interoperability in the field. The success of such cross-vendor testing may benefit from incentives to encourage endpoints to participate and to share the nature of the issues they identify, as attaining sufficient participation is the most anticipated barrier to obtaining and utilizing this information. By bringing together EHR developers to discuss real data, a more consensus-driven approach to the practical issues of implementing the C-CDA standard may be achievable.

It is important to note that there is a reluctance by some vendors to share EHR-to-EHR interoperability information. Ideally the EHR consumer—and likely the US government and US citizens who have paid for interoperability capability—would like to see a matrix including all major EHR vendors, reflecting every EHR’s ability to successfully interoperate with every other different type of EHR, based on actual production exchange.\(^8\) HISPs are motivated to share their HISP-to-HISP interoperability success for business reasons, but EHR vendor endpoint customers appear not to be similarly motivated. EHR-to-EHR interoperability would be most accurately assessed by production endpoints.

\(^8\) Testing of both different payload types during EHR certification would not likely be the most comprehensive measure of this capability, but could serve as a starting point. This data would be the most useful if it reflected actual field testing.
Though all systems are required to certify for their ability to accomplish Vanilla Direct transitions of care, endpoints can also optionally be evaluated and certified for their ability to create and transmit or receive and incorporate a payload in XDM Zip file format (a Zip file containing a C-CDA plus other metadata attached to a Direct message). This disconnect between what is allowed in attestation by a sender (XDM or simple C-CDA attachment) and what is required for certification as a receiver (only simple C-CDA attachment) has created an unintended potential for optionality that represents the second part of content/payload related interoperability challenges in the field.

For example, systems which have certified their Direct receiving technology for only the simple C-CDA attachment standard may not be able to consume a C-CDA received within an XDM Zip payload, and would therefore be incapable of understanding a message received from a sender who deploys only the optional XDM payload in production, unless and until the receiver systems enable functionality to consume the XDM Zip format. In current practice, such systems may make these Zip files available for manual processing or may simply discard them as invalid payloads.

Furthermore, many EHR systems have certified for an additional optional transmission standard known as XDR, which is a SOAP-based protocol. An XDR-enabled EHR may partner with an XDR-enabled HISP to provide a SOAP-to-Direct gateway, whereby the C-CDA document and metadata transmitted in the XDR message are converted to a Direct message for delivery to the final destination by the HISP. The XDR and XDM for Direct Messaging Specification (referred to in this report as the “XDR/XDM Specification”) is referenced in the 2014 Edition Standards and Criteria Final Rule and followed for EHR certification. It defines a method for a HISP to convert the XDR message into an XDM payload to be sent via Direct. Thus, XDR-enabled EHRs may encounter the same issues when sending to systems that cannot process XDM as EHRs that natively transmit XDM payloads.

The generalized, payload-specific interoperability matrix shown in Figure 4 further illustrates the payload incompatibility issue: when an “Optional XD*” system (either native XDM or XDR converted to XDM by a HISP) sends XDM Zip files to Vanilla Direct endpoints that only understand C-CDAs as attachments, those endpoints exhibit varying behaviors. According to preliminary feedback, in general, they typically do not positively acknowledge message receipt via Processed MDN, nor can they view or incorporate the payload, and we are left to speculate that this occurs because the anticipated MU2 C-CDA XML payload is not attached in the format preferred by the receiving system. This combination of sender/recipient behavior is indicated by an orange square in the upper right cell in Figure 4. When a simple Vanilla Direct sender’s XML payload is sent to an Optional XD* system, the receiving systems may or may not recognize and incorporate the XML, and this is again indicated by an orange square in the lower left cell in Figure 4. The other send/receive pairings are compatible, by design.

---

9 Observed responses to this situation include, for example, not sending any MDN, sending a Processed MDN followed by a failure DSN, sending an immediate Failed MDN or DSN, and sending a Processed MDN but not enabling file unzip and incorporate at the endpoint.

10 Although this works some of the time, likely in part because it is required as part of certification testing, anecdotal information suggests the process of assembling the C-CDA Only payload into an XDM Zip cannot always be completed reliably due to the XML occasionally being insufficient to generate the XDR. Future use cases in which an XML dataset would not necessarily be part of a payload are also anticipated, and these use cases would not ever be sufficient for generation of an XDR message.
### Interoperability by Payload Type

<table>
<thead>
<tr>
<th></th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sender</strong></td>
<td><strong>Recipient</strong></td>
</tr>
<tr>
<td>XDM</td>
<td>Optional XD*</td>
</tr>
<tr>
<td><strong>Vanilla Direct</strong></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4 shows Interoperability by sender Payload Type and recipient capability. The two different Direct payload types possible in certification and attestation are shown in blue as rows and columns of the grid at top. Certification-tested exchange patterns which are typically successful at the container level are shown in green. Exchange patterns not tested during certification but known to exist in the field due to attestation rules are shown in orange.

DirectTrust recognizes XDR as an edge protocol that generates MU2-compliant Transition of Care messages, and many Direct HISPs support this edge protocol and will repackage the XDR transmission as an XDM Zip payload attached to a Direct message. Therefore, receiving endpoint systems are encouraged to support XDM Zip as a Direct payload for receiving data as part of this use case. Rejection of an XDM payload is not technically out of compliance for endpoints who have certified exclusively for “C-CDA Only” send and receive capability; however, the result is limited interoperability. Some contend that a receiving HISP is in the best position to convert and deliver the payload in a consumable format to an edge system in this case. Based on this rationale, workarounds wherein a sending or receiving HISP “unzips” data on behalf of an edge system to extract the C-CDA have been unofficially supported by some HISPs at the behest of customers who would otherwise be unable to meet MU2 attestation requirements due to payload incompatibilities, but these solutions are outside of any standard or specification. Others contend that this practice is entirely out of scope for the HISP as a transport provider, or is at odds with the goal of establishing a standardized set of edge protocols with which EHR systems may interact with HISPs.

Ideally, a received XDM Zip attachment should be delivered by a receiving HISP to an end system in its entirety, and processing of the Zip file should take place at the end system level. An exception to this is the special case where XDR is used as the edge protocol for communication between the HISP and the EHR system, where repackaging of a received XDM Zip file as an XDR transmission should be performed by the HISP in accordance with the XDR/XDM Specification. Unpacking or “exploding” of XDM content by a receiving HISP is not formally encouraged at present, as there is no standardized method to do so. To expedite interoperability, a minimum implementation guide to bootstrap the use of XDM Zip payloads by edge systems for the most common use cases would therefore be helpful.

It should be noted that, similarly to the versatile MIME standards for email, the XD* standards allow for arbitrary content to be included in an XDR transmission or included in an XDM Zip file, and are not
limited only to the MU2 transition of care use case. The existing XDR/XDM Specification allows for Direct messages containing MIME attachments, with or without a C-CDA, to be prepared reliably for transmission from a receiving HISp to an XD* endpoint. However, some XD* edge systems will reject XD* containers that do not contain full metadata or contain content other than, or in addition to, a C-CDA XML document, or will ignore other attachment types that may be included in the XD* container. Because the conversion of the C-CDA Only payload to an XDM Zip has been standardized, it is recommended that Optional XD* endpoints fully support the limited XD metadata resulting from the conversion process defined in the XDR/XDM Specification.

In the other direction, for messages originating from a sending Edge system, a HISp should repackage XDR transmissions received from XDR edge clients as XDM attachments in accordance with the existing XDR/XDM Specification, which includes a consensus-based conversion algorithm from XDR to XDM. As a workaround, and upon the explicit request of an XDR client, some HISPs have provided an alternate repackaging scheme for XDR data in order to attach C-CDA XML documents directly to outbound Direct messages rather than within an XDM Zip file, for transmission to recipients with limited or no support for XDM payloads. However, as such alternatives are not standardized, assume a specific use case, and may result in the loss of metadata, directory structure, or other information included in the XDR transmission, they should be used only as a temporary measure.

Another factor complicating XDM transmission is the choice of MIME type to identify the attachment. To facilitate interoperability, DirectTrust recommends that all senders of XDM Zip attachments label the attachment with the MIME type application/zip. Recipients should examine attachments labeled as either application/zip or application/octet-stream for potential XDM content, however, as the latter MIME type is also encountered in the field.

In addition to the 170.314(b)(1) and (b)(2) transitions of care payloads, the other payloads systems may receive are the C-CDA and human readable versions thereof, as part of 170.314(e)(1), View/Download/Transmit. Certification standards are more flexible for this measure, and may include, for example, PDF, HTML, and XML+XSL as the human-readable file types. This use case introduces situations in which EHR summaries of care may be sent to provider recipients in many different potential file formats that the receiving systems are not necessarily prepared to accept. Evaluation of these payloads has been studied even less than that of (b)(1) and (b)(2), however it will require similar guidance on payload restrictions moving forward in order to optimize interoperability.

Examples of additional content/payload-related practices which hinder interoperability include:

- Accepting messages that contain a text part or a payload attachment, but not both
- Accepting only messages that contain an MU2 payload (again, not necessarily non-compliant, but preventing communication via Direct beyond the transitions of care use case)
- Expecting the text part before the C-CDA (or not accepting a message if sender adds message parts out of the expected order)
- Use of application/octet-stream as attachment type: the DirectTrust Security and Trust Compliance workgroup has determined that this attachment type is not sufficiently specific for the MU2 use case and its use is generally discouraged, but in the field some XDM Zip files are so tagged and attachments of this type should be examined for an MU2 payload.
- Sending a payload referencing a proprietary, privately-hosted, or unconventionally-named style sheet which may not be universally accessible due to recipient’s firewall settings or may introduce security risks to the recipient
- Sending broken or invalid HTML as part of the XDM container, the message body itself, or one of the attachments, potentially making the content non-viewable by some recipients
- Self-imposed C-CDA or other structural data or metadata validation causing receivers to accept too narrowly—such that C-CDAs or XDM Zip files that would have been declared valid by certification testing are not incorporated or entire messages are dropped

These practices are discouraged since they are inconsistent with “sending narrowly and receiving broadly”, a principle which is known to play a critical role in achieving good interoperability, and that is often stressed in the DirectTrust Security and Trust Compliance workgroup.

It is expected that use cases for additional payloads will be common in Direct Exchange in the coming years, since C-CDA XML and XDM Zip files are impractical as a universal payload for every possible use case. The purpose of introducing Direct as a required transport protocol was not likely intended to facilitate only the two required use cases. At a minimum, as an optional transport protocol for secure messaging between patient and provider, Direct is intended to serve as an infrastructure for more general healthcare communications as well. The C-CDA and XDM Zip do not lend themselves well to simple text messages nor to messages with only simple image file attachments, which would be natural next payloads to send, and in some use cases are being sent already.

Recognizing that the C-CDA XML and/or XDM Zip will not be practical containers for all content exchanged via Direct in future use cases, it would be helpful to establish a few additional payload types that must be or may be accepted as part of certification testing and/or field confirmation. Payload types should be consumable without intervention by the end user, and their use should be demonstrated by actual software deployed in the field. Modular certification for transmission and utilization of additional payload types, or a refined list of existing types, should be offered over time—with some payloads being required and some optional. Key to end user benefit and interoperability in the field will be a vendor’s ability to transparently provide and communicate these capabilities to their customers. For example, certification documentation should enumerate any optional payload types which were certified and will be supported by the product when deployed in the field.

These behaviors observed in the field additionally demonstrate that it is under-specified how to communicate back to the sender whether a payload will or will not be processed (Viewed? Incorporated? If not, why not?). It is therefore not clear whether the sender should retry sending the message or not, and what, if any, modifications to the payload might be needed prior to re-sending. This ambiguity should be considered when re-evaluating the current MDN specifications.
3  **INTEROPERABILITY CHALLENGES AND SOLUTIONS: HEALTH INFORMATION SERVICE PROVIDERS (HISPs) AND SECURITY/TRUST AGENTS (STAs)**

The Direct specification itself is well-understood, but there are a few places where the most common and most impactful message handling issues occur. This section catalogs the most frequent pitfalls which hinder interoperability but can be easily and reliably managed now that they are well documented.

**Message Digest**

The message digest is the critical element of a digital signature used to confirm that the content has not been altered in transit. However, improper computation and/or validation of the message digest is an issue that occurs in the field. The recipient should re-compute the message digest from the data they have received and compare it with the digest computed by the sender that was included in the digital signature. Interoperability issues may arise when a HISP does not perform this digest evaluation properly, since it is possible to exchange with others while skipping this required step, perhaps unknowingly through improper STA design. Encoding and canonicalization issues relating to line breaks in certain MIME types may cause some faulty implementations to miscompute digests only for certain messages.

Not strictly validating the message digest may be a way to work around digest miscomputations by the sender and/or recipient. However, HISPs that do not evaluate the message digest risk potential data integrity issues and are not compliant with the Direct specifications. Furthermore, when a receiving party does not independently confirm the message digest, they are vulnerable to spoofing attacks and may unknowingly accept arbitrary content that has been substituted by a malicious party that is reusing an otherwise valid signature from a third party. Although validation of the digital signature is a required element of a strong security and trust framework, this criterion is difficult to enforce in the field, due to the subtlety required to detect noncompliance. Incorporating negative test cases with intentionally miscomputed digests into certification testing may help to identify non-compliant systems.

**Message Wrapping**

Wrapping of a Direct message provides integrity protection for message headers, which are otherwise outside of the digitally signed portion of a message and not included in the computation of the message digest. Direct messages can be wrapped or unwrapped, and message wrapping is not currently required for certification. However, wrapping outbound messages and the ability to receive a wrapped message are now required within DirectTrust, to mitigate the risk of message headers being manipulated in transit to spoof the sender or recipient address. This risk is limited, in that a message with a manipulated envelope cannot be validated unless the modified sender or recipient also share a domain bound certificate with the original sender or recipient. Revising certification criteria to require wrapping of outbound messages can mitigate the associated risks.

**SMTP Envelope**

Using the NULL sender in the SMTP envelope when sending MDNs is actually compliant with the Direct specifications, but this is rarely encountered in the field because use of the NULL sender has historically
caused problems with certification testing tools, namely the NIST Transport Testing Tool. Most implementations, including the Direct Project’s reference implementations, populate the SMTP envelope with the same Direct address as is found in the RFC822 headers instead of using a NULL sender. Systems that strictly follow the specifications are likely to run into issues if they are unable to handle MDNs without a NULL sender. Therefore, at present, systems are best positioned for good interoperability when they are able to accept MDNs from the occasional STA that does use a NULL sender, but who themselves use the same value as is found in the RFC822 headers when sending MDNs to other systems, even though this is not strictly compliant with the specifications.

Message Disposition Notifications (MDNs)

These acknowledgements are a key aspect of Direct, much like a fax machine’s confirmation that a fax has been sent successfully. A Processed MDN indicates that a message has been accepted by the receiving HISP and that HISP has accepted responsibility to attempt delivery to the final recipient; this MDN is always required. A Dispatched MDN indicates that final delivery was successful; this MDN is optional to request. Receiving the Dispatched MDN does not necessarily mean that the message has been read by the final recipient; there is no acknowledgement serving that purpose at this time. Failure MDNs or Failure Delivery Status Notifications (DSNs) can be used to indicate failure of delivery. As discussed above, it would be useful to indicate the receiving party’s ability or inability to process a payload using MDNs or DSNs, but there is no system-wide mechanism for doing so today. Thus, the communication of failures, especially after sending a Processed MDN, should be further specified and clarified within the Applicability Statement.

Implementation of Dispatched MDNs is not required in order to be compliant with the Direct specifications, so interoperability issues arise when a Dispatched MDN is requested by a sender but cannot be returned by the receiving system because Dispatched MDN capability has not been deployed in the recipient’s system. Although the receiving system may, in fact, be able to deliver the message and incorporate the payload, the sender is left to assume the message transmission has failed in this situation because the Dispatched MDN required by the specification is never received. DirectTrust recognizes the importance of being able to request and receive Dispatched MDNs in certain use cases, and has made it an accreditation requirement that HISPs be able to respond appropriately to Dispatched MDN requests made by senders, enabling senders to receive this confirmation when it is needed and additionally eliminating this type of avoidable failure. All HISPs who do not currently support the final delivery notification mechanism should, at a minimum, update their systems so that they are able to respond appropriately to requests for Dispatched MDNs from counter parties.

In the short term, until support for the final delivery notification mechanism on the receiving side is more universal, requesting Dispatched MDNs too liberally—when additional assurances that the

---

11 Specifically, systems which followed the specification accurately and used the NULL sender would not be able to successfully pass the NIST Transport Testing Tool’s required test cases which examined characteristics of the Message Disposition Notification sent by a system under test, due to the way in which the tool was implemented. This had the side effect of forcing most systems in the field today to be technically non-compliant.

12 See the Implementation Guide for Delivery Notification in Direct.
message has reached its final recipient are not necessary—will increase the risk of avoidable failures since all HISPs in the field are not currently capable of returning Dispatched MDNs. Thus, at this time, HISPs and edge systems should request Dispatched MDNs only in cases where the additional assurances provided by this mechanism are required.

On the receiving side, transmitting a Processed and/or Dispatched MDN too broadly can lead to inappropriate assumptions being made by the sending HISP or the sending edge client. Returning an unsolicited Dispatched MDN to the original sender by the receiving HISP or receiving edge client may have unexpected results, since the sender will not be expecting this response and will not be able to match the Dispatched MDN to a corresponding request. As many STAs will pass such MDNs on to end users, receipt of an unexpected MDN may also be confusing to end users who were not requesting it. Thus, HISPs should not transmit unsolicited Dispatched MDNs.

Returning a Processed MDN to the original sender when the receiving HISP knows that the recipient address does not exist may result in delivery of a subsequent failure notification, with the associated problems discussed further in the next section. A receiving HISP should not send a Processed MDN if the HISP knows that a receiving address does not exist, unless a wild-card or catch-all account exists to manage such messages by a properly vetted end user(s).

A Processed MDN may be returned even when the message payload is delivered but cannot be consumed, which may be misleading to the sending system, and may even lead to failures in care coordination among providers. Examples of payloads that may not be consumed are discussed in Section 2 of this Report and include: a payload type that cannot be processed by the receiving endpoint; an unrecognized attachment type inconsistent with an MU2 payload for an endpoint that expects such a payload; a payload that is otherwise inappropriate for the use case as supported by an endpoint; or a payload that does not validate after being unzipped, where applicable. Some HISPs and edge systems are actively communicating payload-related failure notifications, but this is not yet standardized. Additional clarification on when to return a Processed MDN or the communication of failures after a Processed MDN has been sent is necessary, to eliminate this ambiguity.

Timeliness of MDNs is important. If a Processed MDN has not been received within a period of time established by the sending HISP or sending edge client, then a message will be marked as failed by the sender, even if the message eventually does reach the intended recipient and a subsequent Processed MDN is sent. Many HISPs have adopted a wait time of one hour for this determination as a reasonable default timeout value. In the case where a Dispatched MDN is requested, the message will be marked as a failure by the sender if the Dispatched MDN has not been received within the prescribed time

---

13 One example of where Dispatched notifications may be required is in the case of lab results reporting for Clinical Laboratory Improvement Amendments (CLIA).

14 i.e. not application/xml, application/zip, or application/octet-stream containing an XDM Zip file.
period. To reduce timeout failures, HISPs should transmit a Processed MDN once the STA has determined the message is trusted and passes integrity validation.

Some HISPs have cited the Applicability Statement assertion that sending a Processed MDN constitutes accepting responsibility to deliver a message as a reason to delay transmission of the Processed MDN, sometimes until after the recipient reads the message. The Applicability Statement should be clarified to indicate that the transmission constitutes acceptance of responsibility to attempt delivery and that a HISP should send subsequent failure MDN or DSN if the delivery attempt is unsuccessful.

Similarly, some HISPs or edge systems may define final delivery as the time at which a message is read by the intended recipient. To reduce timeout errors related to Dispatched MDNs transmitted after the sender’s timeout interval has expired, HISPs and edge systems should define final delivery as the time at which transport is complete and the message is available in the recipient’s mailbox or equivalent endpoint from which the intended recipient will access the message, rather than the time at which the recipient views the message.

For edge protocols where edge systems poll the HISP for incoming messages, interoperability problems may arise when a receiving HISP waits for polling by the edge to determine when Dispatched or Processed MDNs are to be sent. If polling is infrequent, these MDNs may be sent after the sender’s timeout interval has elapsed and after the message has already been marked as a failure on the sending side. Thus, HISPs and edge clients should establish appropriate polling intervals to reduce the likelihood of such timeouts occurring.

MDN-related issues may also surface due to a lack of diligence on the part of the HISP operator in troubleshooting at the mail server level. Unexpected or irregular content in the MDN header may cause the HISP to not process a received MDN because it cannot be successfully parsed. Early interoperability testing by DirectTrust demonstrated that subtle variations in MDN content such as the presence or absence of a space character between fields in the MDN report could cause certain STAs to drop the MDN altogether as invalid. To achieve greater interoperability, HISPs should implement MDN processing which tolerates such variations.

**Domain-bound certificates and wildcard addresses**

Returning a Processed MDN when the destination address does not exist or has been terminated may cause problems, even if a subsequent failure notification is sent. This may occur in the setting of a domain-bound certificate where management of individual addresses is handled by the edge client, and the HISP STA forwards all messages for that domain to the edge without knowledge of whether a specific address in the domain exists at the edge.

Many HISP and/or edge systems will handle a delayed failure such as subsequent rejection of a message by the edge client by sending a Failed MDN or Delivery Status Notification (DSN) at the time that the subsequent failure occurs. However, the Direct specification does not provide a mechanism for the

---

15 This may also be a matter of local policy, and many systems strive for Dispatched MDN confirmation within 5 minutes, but in general the one hour time frames have been widely accepted as a default maximum time allowable for these notifications to be sent.

16 Examples of edge protocols used for polling include POP3, IMAP, and some custom edge APIs.
confirmation of receipt of such delayed failure notifications, and unlike the initial Processed MDN, the original sender is not expecting it as a guaranteed part of the protocol, so there is no way to be certain that the original sender ever receives it. For example, if a delayed, Failed MDN or DSN is lost in transit, there would be no way for the original sender to know it was sent by the recipient or the recipient’s HISP, nor for the recipient to know it was not received by the original sender. Extending the Applicability Statement to address this limitation would improve the robustness of these delayed notification mechanisms.

4 INTEROPERABILITY CHALLENGES AND SOLUTIONS: CERTIFICATION AUTHORITIES

Certification Authorities (CAs) issue X.509 digital certificates which make Direct exchange possible by binding the identity of the network participants to their digital keys. Relying parties who trust the issuer can make use of the certificate to encrypt messages or validate digital signatures. The following characteristics specific to digital certificates, at the core of securing the Direct address itself, have a critical impact on interoperability.

Certificate structure

Variations in certificate profiles across HISPs introduce interoperability issues that can sometimes be resolved by the relying party becoming more tolerant, by the certificate issuer becoming more compliant, or by the trust community adopting a uniform certificate policy addressing common issues.

Examples of CA practices that lead to interoperability problems include:

Omitting or not properly populating the Authority Information Access (AIA) extension of a certificate such that a relying party does not have sufficient information to build a certificate chain from an end entity certificate to an issuing CA when intermediate CA certificates are not known to the relying party.\(^{17}\) The Applicability Statement currently recommends inclusion of AIA information but could be revised to require it in cases where intermediate CAs are used.

Publishing end entity certificates which do not contain a Subject Alternative Name (SAN), or which contain SAN information that does not match the Direct address or Direct domain. Strictly, such a certificate does not meet the requirements of the Applicability Statement; nonetheless, such certificates are encountered in the field. All trust communities should require, at a minimum, conformance with the Applicability Statement.

Preventing these issues in the field is challenging, because actual certificates used during certification testing or as samples shown prior to admission into a trust community may be different from those used in production, or multiple profiles may be in use by individual CAs. Furthermore, those relying parties who expect stricter compliance from issuers are at greater risk of having their own customers

\(^{17}\) Not being able to read and use AIA information is a limitation of early versions of the Java Reference Implementation of which HISP operators should be aware.
experience interoperability issues. This can also be mitigated by trust communities defining uniform certificate policies for their members.

**Revocation Status Information**

One significant feature of X.509 certificates is the ability of a relying party to reliably determine the revocation status of a digital certificate. This information may be provided as a Certificate Revocation List (“CRL”, a list of certificates that have been revoked and should no longer be trusted), or by offering an Online Certificate Status Protocol (OCSP) responder. Current revocation status information is useful because it provides added assurance that an endpoint is still active and has not been compromised. Providing such information is not a requirement of the Direct specifications, but it offers additional security to those who have agreed to share revocation status information. All DirectTrust Certification Authorities (CAs) are required to publish a current CRL, and may also offer OCSP responders.

CAs that do not publish any revocation data, do not reliably publish a new CRL prior to the expiration of their current CRL, or provide only intermittent OCSP service create discontinuities in the security and trust framework. When revocation status information is unavailable or is out of date, a sender or recipient may experience unexpected interruptions in service when a relying party requires current revocation status confirmation as a precondition of trust. Of greater concern, delivery of a message to a counter party whose encryption and signing keys have been compromised is possible when revocation status information is not available at all or is out of date. Trust communities can mitigate these risks by requiring issuers to make certificate status information available.

Since many Direct certificate issuers outside the DirectTrust network do not provide current revocation status information, and even those who do so often allow their CRLs to lapse, many HISP operators do not require strict revocation status checking in production, in order to enable greater interoperability through minimized interruption in service, opting instead to allow trust when revocation status is undetermined or unknown. To maximize the security benefit of revocation status publishing, CRL or OCSP checking should be performed by a relying party to confirm the status of any certificate that includes a revocation status CRL or OCSP link. The side effect of this requirement is to break interoperability for relying parties when the revocation status information is unavailable or out of date, so trust communities who require publication and use of certificate status information should also require high availability and timeliness of publication.

**Mixed use domain**

Using a combination of domain-bound and address-bound certificates at a single domain/subdomain or at a subdomain for which the parent domain uses address-bound certificates is not prohibited, but may lead to unpredictable behaviors. For example, a cached domain-bound certificate may be used inadvertently by a counter party when an address-bound certificate is also available but is not cached. Implementers are advised to be aware of related technical and policy issues when deploying this certificate usage model, and care should be taken to avoid collisions between address and domain bound certificates. Trust communities can mitigate these problems by restricting the use of mixed use domains.
5  INTEROPERABILITY CHALLENGES AND SOLUTIONS: ON THE WIRE, BETWEEN HISPs

DNS, LDAP, and SMTP servers

Obstacles to interoperability occur when a HISP’s DNS servers, LDAP servers, mail servers, or the Direct software itself is not properly monitored and managed. Intermittent server issues are often difficult to diagnose and may result in unexplained failures. DNS data is often cached at multiple locations, so some DNS failures may go unnoticed, at least for some users, and corrections to DNS errors may take time to propagate to all endpoints. Some DNS records are incomplete or misconfigured, such as missing mail exchanger (MX) records for Direct domains that are in active use, in which case mail is receivable from the associated addresses but messages, including MDNs, cannot be delivered back to these addresses. Regular monitoring of server status by operators and validation of DNS records may help mitigate these types of problems.

Trust

Interoperability is not possible until mutual trust has been established by the sending and receiving HISPs. Trust configuration can be a source of interoperability issues when bundles are not being loaded or updated properly by the bundle publisher or by a HISP, are not reliably available, or if a sender and recipient are not part of the same trust community. To optimize interoperability at scale, HISP operators should participate in a trust community that eases the scalability challenges of establishing trust—which can otherwise be both technically and operationally burdensome. DirectTrust has elevated this practice by establishing the use of a single Federated Services Agreement for its participants, and by publishing trust bundles, instead of relying on multiple one-off agreements and disparately-hosted trust anchors. Trust community operators who offer trust bundles should reliably publish updates and define a minimum recommended interval at which members should check for changes.

6  INTEROPERABILITY CHALLENGES AND SOLUTIONS: MANAGEMENT ISSUES

Trust

As suggested in the previous section, trust also involves matters of policy. Establishing trust with a counter party is a mature aspect of HISP management, the basic capabilities of which are demonstrated during certification testing. Mutual trust must be established before interoperability is possible. However, policy aspects are also important in the field to determine what endpoints a HISP or edge client will or will not trust. Interoperability may be challenging if a HISP is not part of a trust community such as DirectTrust that provides a trust anchor certificate bundle for seamless management of trusted anchors as an alternative to maintaining a collection of individual anchors and one-off HISP-to-HISP trust agreements.¹⁸  Contrary to what some may assume, DirectTrust does not restrict which counter parties

¹⁸ See the Implementation Guide for Direct Project Trust Bundle Distribution for additional information.
member HISPs or endpoints may or may not trust. Trust communities should not prohibit members from enabling trust with endpoints outside the community.

Most Direct participants expect to be able to send from their Direct address to any other known Direct address, just like they would an ordinary email message.

Some providers do have concerns about receiving information from certain Direct addresses, especially when little or no identity proofing\(^{19}\) has been performed, when endpoints are not required to abide by HIPAA, when addresses are issued to patients, or when endpoints use self-signed certificates or their data handling, certificate, and system management have not been accredited. Trust capabilities should be clearly communicated to end users, so that trust issues and their potential resolution can be better understood and any foreseeable interoperability issues anticipated and addressed.

**Product Management**

Some Direct operators impose restrictions that go beyond the MU2 requirements and the Applicability Statement. This small class of issues are unrelated to technical problems per se, but are rather product communication issues between vendors and end users of Direct messaging. These issues present as somewhat of a nuisance to providers.\(^{20}\) Examples include the following:

1) Customers may not have control over the trust settings for their own address(es) or are not aware of their trust setting choices. Some HISPs may enforce whitelisting above and beyond bundle anchor whitelisting (and other than as requested by a customer), or otherwise limit trust enablement with other, Direct-compliant counter parties with whom a customer has a business need to exchange.

2) Excessive requirements can be made by a counter party HISP with whom trust is being attempted—such as requiring that parties be listed in a local directory with the counter party HISP or EHR vendor—a sort of local whitelisting—as a prerequisite to interoperability. This is generally regarded as a barrier to interoperability since seamless interoperability by virtue of the trust anchor exchange alone.

3) Enforcing case-sensitivity for a Direct address either in the message headers or when listed in XD metadata is another example of a design choice that leads to an inability to process some messages. Direct addresses and Direct domains belonging to its own customers should be treated in a case insensitive manner by a receiving HISP, as is best conducive to interoperability.

4) DirectTrust defines specific policy Object Identifiers (OIDs) to identify the Level of Assurance (LoA) to which identity vetting was performed for users of a particular X.509 certificate. These OIDs are expressed in the Direct certificates themselves and are thus readily available to relying parties. At this time, there is limited support in the field to parse these LoA OIDs and present the LoA information offered to a counter party reliably. Further, the identity of the individuals who have

\(^{19}\) Identity proofing, identify verification, and identity vetting are herein used interchangeably and mean the same thing.

\(^{20}\) This is an observation from direct experience with customers of several HISPs, which we will qualify by saying that the minimum bar for exchange on the part of providers seems to be either DirectTrust accreditation or that the counter party is someone with whom the provider is already doing business—e.g. a referring provider.
been identity vetted are generally not expressed in the Digital Certificate, so there is a disconnect between the reason for performing this identity vetting and relying parties’ potential use of it. Trust communities should encourage members to implement the tools necessary to make use of such information when the community feels its inclusion is of value.

**Identity Vetting**

Each organization participating in Direct exchange may determine its own minimum requirements when selecting the trust communities in which it will participate or which HISP to use. One of the commonly discussed requirements is identity vetting. Identity vetting requirements stipulate the baseline at which participants are identity proofed before being authorized to send or receive Direct messages using a specific Direct credential. Organizations are required by the trust community to allow only appropriately vetted end users to use the credential. This allows every use of the credential to be traced back to an individual whose identity has been verified to the minimum standard required by the trust community.

Differences in identity vetting requirements between sender and recipient may lead to failed communication if the two parties do not belong to a common trust community or one of the parties does not trust the other because the parties are operating at different minimum identity assurance levels. ONC has established a baseline recommendation of LoA-3 identity proofing for providers. Interoperability between providers can be improved if all provider organizations and provider trust communities adopt this recommendation. It is for this reason that the DirectTrust Accredited Trust Anchor Bundle requires LoA-3 identity verification.

The identity verification process is communicated to and understood by end users of Direct at varying levels of completeness. Gaps and inconsistencies in identity vetting processes by a trust community limit the value of that network to relying parties who are demanding a consistently high bar of identity assurance, and who may then choose not to exchange with that community.

Every end user of a Direct address\(^{21}\) is required by DirectTrust to have their identity verified either directly by a DirectTrust Registration Authority or by a Trusted Agent of the Registration Authority. A valid Trusted Agent proofing process is substantively identical to the verification process that would otherwise be performed by the Registration Authority, except that part or all of the process is performed by a party other than the Registration Authority, such as a Notary or the end organization itself. When a trust community defines its identity vetting requirements, the vetting procedures should be the same for any person who can use a Direct mailbox, whether they are assigned to an address- or domain-bound certificate, or whether that certificate is issued to an individual or an organization, since most Direct implementations will treat these different combinations of users and certificates in the same manner when validating trust with the corresponding endpoints.

**Other onboarding logistics**

Individuals or organizations tasked with choosing their own HISP may not understand the implications their choice of HISP may have on interoperability. Transparency regarding HISP policies, available trust

---

\(^{21}\) This means any person who can send or receive a Direct message using a Direct mailbox.
7 Recommended Changes to Existing Specifications

Methods of enhancing the Applicability Statement and associated implementation guides and specifications to ensure more reliable interoperability

Recommended changes to the Applicability Statement discussed in this Report include clarification of the meaning of a Processed MDN. Transmission of a Processed MDN should indicate that the receiving STA is taking responsibility to attempt delivery to the specified recipient, rather than responsibility to deliver, and that receipt of a Processed MDN does not guarantee that final delivery was made. It should also be clarified that the existing final delivery notification mechanism should be used when such a guarantee is required. In conjunction with the above, the notification requirements and mechanisms when message delivery does not succeed, including notifications that may arise after an initial Processed MDN is sent, or when message payload cannot be processed, should also be clarified. Cases where a message contains more than one payload or payload type, and not all content could be understood, should also be considered.

Additionally, the use of the AIA extension in Direct certificates should be upgraded from a recommendation to a requirement, at least for certification hierarchies that include intermediate Certification Authorities that may not initially be known to counter parties.

Guidance should also be provided to those who have a need to convert from an XD* container (an XDM Zip file or an XDR transmission converted to XDM) to a MIME container by publishing a new specification for conversion or an update to the existing XDR/XDM Specification, to complement the method for conversion in the reverse direction from a MIME container to an XD* container that is already described in the XDR/XDM Specification, and providing examples of when the use of this conversion is needed. This recommendation should include consideration of the possible variety of transport offerings in the field, and should provide any guidance that is lacking to ensure bidirectional interoperability between every certified EHR and every other certified EHR.

Enhancing the certification testing program

Existing certification criteria as well as development methodology for future criteria should be revised so that any Direct payload type that is allowed for a particular use case, even if optional for sending, is always mandatory for receiving, in order to close the existing payload requirement gap and prevent new ones from arising in the future.

The minimum viable Direct payloads that should always be accepted by Edge systems for the existing transitions of care use case include both a C-CDA XML attachment and an XDM Zip file containing a C-CDA XML attachment, where the payload also meets the requirement for certification. Additionally, all XD* endpoints, including those endpoints using XDR as an edge protocol to communicate with a HISP, should be able to accept a C-CDA XML document within an XD* container that has been converted from a MIME container following the method specified in the existing XDR/XDM Specification, even if
complete XD* metadata is not available. The following endpoint system actions are also recommended for certification:

<table>
<thead>
<tr>
<th>Message File Types Common in the Field</th>
<th>Recommended Endpoint System Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more of the following attachments:</td>
<td>1. Send a Processed MDN when message is otherwise compliant and deliverable</td>
</tr>
<tr>
<td>C-CDA</td>
<td>2. Provide ability to incorporate the clinical data in the C-CDA</td>
</tr>
<tr>
<td>C-CDA + XSL</td>
<td>3. Publish consumable container types</td>
</tr>
<tr>
<td>Any of the above plus a text part</td>
<td></td>
</tr>
<tr>
<td>Attachments may be in either an XD* or MIME container.</td>
<td></td>
</tr>
</tbody>
</table>

| Other attachment types that could be included in the above containers: | 1. Send a Processed MDN when message is otherwise compliant and deliverable |
| PDF                      | 2. Provide a method for viewing each consumable attachment type |
| HTML                     | 3. Publish consumable attachment types |
| Other human-readable     |                                    |
| Any of the above plus a text part |                                    |

Revise existing certification criteria and development methodology for future criteria that enable cross-vendor interoperability to include an ongoing interoperability testing and improvement component for maintenance of certification, as discussed further in the next section.

Enhance certification testing tools to include additional negative tests to confirm that the message digest is evaluated properly, revocation checking is performed, CRLs are discoverable and properly formatted, and that systems are tolerant of the common variants in the message or MDN structure described in this Report.

Further constrain required C-CDA elements for current use cases. If optional elements are allowed on the sending side, they should also be constrained and all certified systems should be required to consume received documents containing both required and optional elements, i.e. all receiving systems must be able to understand all required and all optional elements.

Require certification testing labs to collect and make available the C-CDA and XDM samples generated by systems under test during certification testing and to make these samples publically available to other EHR developers.

Revise existing certification criteria to require support for the Direct final delivery notification mechanism. At a minimum, certified technologies or their HSPs should be able to respond appropriately with a Dispatched MDN or failure notification to counterparties that request final delivery notification.
8 **RECOMMENDED BEST PRACTICES FOR THE NEXT PHASE OF DIRECT EXCHANGE**

Two points of data conversion will need to be specifically addressed in more detail in order to resolve the gap in payload compatibilities: baseline C-CDA Only messages sent to XD* Only systems and XDM messages sent to C-CDA Only systems. Standards should be enhanced as described in the previous section, and systems made more accepting of converted payloads, to bridge this gap, as outlined in the following table.

<table>
<thead>
<tr>
<th>Send/Receive Capability Currently in Production Use by Edge System</th>
<th>Recommended Future Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIME container only via SMTP; no XDM support</td>
<td>Add support for converting XDM Zip attachments, natively or via HISP, according to the new or updated conversion specification described above, and potentially other attachment types, or add native XDM support</td>
</tr>
<tr>
<td>Optional native XDM directly to/from EHR only, via SMTP</td>
<td>Add support for C-CDA receipt within a MIME container, and potentially other attachment types in either XDM or MIME container</td>
</tr>
<tr>
<td>Optional XDR only, via XD HISP</td>
<td>Edge systems should be more flexible regarding inbound message payloads, possibly tailored to specific use cases, and accept MIME containers converted to XD* containers by the HISP according to the existing XDR/XDM Specification, even if complete XD* metadata is not available</td>
</tr>
</tbody>
</table>

Regular interoperability testing with counter parties and inclusion of interoperability testing in the software development process have been recommended by DirectTrust to its members, and the success of the HISP-to-HISP DirectTrust network has benefitted from the implementation of these recommendations. Thus, an ongoing Direct cross-vendor testing requirement is recommended in order to ensure continued successful interoperability for all users of EHR systems. This could be structured as a maintenance of certification program administered by trust communities or other industry groups. Endpoint testing would consist of participants transmitting the C-CDA variants that they use in the field to many receiving systems utilizing EHR technology developed by different vendors. This could be coordinated by the administrating organization or through a tool similar to the NIST Randomizer Tool.

Demonstrating an ongoing commitment to end-to-end testing as well as a minimum baseline of successful real world interoperability could become a condition of maintaining certification, and communications with counter parties and customers regarding interoperability, including real world data such as presented in an interoperability matrix, should be required. This data could be published by the organizations administering the cross-vendor testing programs.

EHR endpoints should each publish technical contact information specifically intended to facilitate resolution of interoperability issues related to transport or content incompatibilities, as DirectTrust HISPs have done for their transport services. Without this step, it is cumbersome for a counter party
EHR vendor to attempt to troubleshoot payload issues with the customer on the other side of the exchange.

System operators should enable and maintain controls for monitoring and addressing system reliability issues. Current service demands require that DNS, LDAP, certificate status, and SMTP servers are highly available, are correctly configured, and operate correctly under expected loads. Trust communities should include requirements for service reliability in their participation criteria.

Currently, ambiguities in the specifications exist as to expected behavior when a Processed MDN is returned by a HISP prior to the Edge system evaluating the message payload received. Edge systems should be able to evaluate their endpoint’s capability of processing incoming data from trusted senders by both examining the payload contents and evaluating the addressee, such that the system can return a meaningful failure notification to the sender when applicable, such as when processing of a payload fails unexpectedly or a recipient does not exist or has been deactivated. This would remove the ambiguity on the sender side in determining whether an unsuccessful transmission should be retried or if resending would also fail. Meaningful failure notifications would streamline follow up with the recipient’s EHR or HISP interoperability contacts to address the precise nature of the incompatibility. The ability to provide a meaningful failure notification should be incorporated into edge protocols used between Edge systems and their HISPs.

Direct has proven its relevance as a platform for reliable, reusable trust networks for the exchange of health information, without the need to create multiple point-to-point secure connections or to configure multiple interfaces for every different exchange participant. New interoperability use cases for Direct should be developed wherever secure cross-vendor exchange is needed. Additionally, the security and trust framework established for Direct should be leveraged in the development of other cross-platform APIs where the Direct transport model cannot be applied. We expect that emergent “pull” paradigms, for example, will encounter the same types of payload and trust challenges that the Direct community has already addressed, and that reusing components of the existing Direct infrastructure where possible will lead to greater interoperability for all.

9 CONCLUSIONS

Interoperable Direct messaging occurs today in a thriving ecosystem populated with over half a million Direct addresses, and is growing rapidly. The backbone of this network is well-established, and is now in the fine-tuning stages. The promise of secure cross-vendor healthcare data exchange is now close to fulfillment, with a few “last mile” payload consumption hesitations being the only things standing in the way of healthcare data liquidity over a robust national data exchange infrastructure.

Most EHR technologies are by now equipped with the capacity to securely exchange patient data using Direct. Although several technical pitfalls have been presented and discussed in this Report, that class of issue is easily identified and addressed in the field—especially where large trust communities convene to perform real world cross-testing and use their collective learning to build a more robust ecosystem by identifying and addressing issues that may not manifest during certification testing. A few clarifying stipulations are expected to help mitigate the major remaining issues: a transport container
compatibility gap and under-specified data payload standard. Some workarounds to address these issues are being evaluated in the field. However, in this environment where many vendors will only take action in response to specific regulations and standards regarding the handling of Protected Health Information, systems will become even more interoperable when current regulations and standards are clarified.

Though many different issues are discussed in this Report, we should be clear about one thing: there is simply no excuse for lack of interoperability. There are plenty of reasons why implementing cryptographic software is challenging, but there are no policy, technical, or cost barriers that should prevent successful, large-scale adoption and interoperability of Direct. A Direct connection to a HISP is reusable and scalable, and a more cost-effective healthcare interoperability architecture is not known at this time. Further, any similar technology focused on healthcare interoperability would be faced with most if not all of the same last-mile challenges. Any single issue that might arise with Direct is certainly addressable on its own in the field today, however network-wide solutions are known to be more effective in solving interoperability issues at scale.

Through tightened specifications that create a more predictable C-CDA dataset, standardized use of Message Disposition Notifications, and optimized service availability from the industry, we expect to benefit from a more reliable network when our work is complete. By additionally performing and documenting tests of real-world document exchange using production systems as they are deployed in the field, and rewarding successful round-trip payload transfer capabilities that are also well-communicated to provider customers, we seek to demystify the issues preventing exchange and instead be able to address them definitively.

Through its broad collaborative, DirectTrust participants have been in a unique position to assemble the comprehensive list of potential obstacles and solutions discussed in this Report, and it is our objective to educate consumers of Direct on these topics, toward greater understanding and more rapid resolution when they are encountered. The limiting factors to achieving interoperability involve better standardization of the exchanged content itself, and not much more. To improve on this, we need to elevate our willingness to develop a common payload, and collaborate in refining the specifications needed to achieve data liquidity, in order to modernize the data management associated with providing healthcare services, as we have already done for nearly every other sector of our economy.

This network is open for business; vendors simply need to make the best use of it by implementing a few technical finishing touches, and utilizing the lessons learned from interoperability testing and real world payload consumption experience to deliver their services with optimal operational interop savvy.