Project Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes a number of requirements on the healthcare industry, intended to simplify and lower the cost of administration. This paper assumes that the reader is familiar with both the HIPAA Transaction and Code Set Regulations Rule and the general approach to electronic messaging embodied in X12 and NCPDP EDI standards.

The WEDI/SNIP Identifiers and Routing project focuses on lowering two of the key barriers to widespread implementation of EDI in healthcare: the cost and difficulty of establishing an electronic trading relationship. Currently, these barriers can be justified for high volume, long term trading relationships, but are seen as a significant detriment to the adoption of standard EDI at the level of small to medium-sized providers (SMP), or providers with large payer bases. Other significant barriers, such as high cost/low availability of EDI-capable provider software, inadequately implemented electronic medical record standards, and general lack of provider awareness/attention to the benefits of EDI are beyond the scope of the WEDI/SNIP Identifiers and Routing project.

This document includes
1) background on the existing Healthcare EDI environment (where we are),
2) the ideal (where we want to go),
3) Identifiers as they relate to routing of transactions,
4) a high-level description of an Electronic Partner Profile,
5) a high-level description of the Healthcare Registry,

6) Examples of how all this would look in practice.

The WEDI/SNIP ID & Routing Project is cooperating with another project, the AFEHCT-WEDI Health Care Communications Security and Interoperability project. The contact page for the project is at http://www.novannet.com/wedi/.

Work Product

This group is a WEDI/SNIP Business Issues SIG (Special Interest Group) for the purpose of developing specifications to address the standard transaction routing problem.

This project will publish implementation guidelines for (1) an Electronic Trading Partner Profile specification to mechanically configure communication and translation software, and (2) automatic "discovery" mechanisms for locating Trading Partners' Electronic Trading Partner Profiles on the Internet, based on their business identifiers.

The Standard Transactions

Electronic Data Interchange (EDI) is founded on principles developed during World War II for improving the communications necessary to transport military supplies. After the War, both government and private industry embraced EDI as a more reliable and cost-effective alternative to the exchange of paper documents used in standard business transactions.

Initially, EDI communications relied on expensive “mainframe” computers and Value Added Networks (VAN), or dedicated, point-to-point connections between trading partners. In the early 1980’s, the personal computer, PC-to-PC dial-up communication, and new file transfer methods made EDI attractive to smaller business organizations. Further standardization of TCP/IP and other Internet protocols has continued to lower financial barriers to deployment of effective EDI systems.

One of the first attempts to globally standardize the process of EDI was the formation of the Transportation Data Coordination Committee (TDCC) in 1975. TDCC focused initially on the transportation industry, later expanding into manufacturing and service businesses. The American National Standards Institute (ANSI) created the Accredited Standards Committee X12 (ANSI ASC X12) in 1979 to manage the growing EDI standards needs in North America. In the late 1980’s, the responsibilities of TDCC were assumed by X12, creating a single U.S. standards body.

During this same period, the United Nations created the Electronic Data Interchange For Administration, Commerce, and Transport or UN/EDIFACT. Literally hundreds of formal EDI standards organizations have been created since then to meet unique business or regional needs. This reflects both the inherent difficulties in getting large numbers of partners to agree to identical message rules, even for similar transactions, as well as the enormous variety of these transactions.

Exchange of standard business documents or “messages” with one’s trading partners is still one of the most important functions in the administration of any business. EDI, and the standardization of product and service nomenclature that normally accompanies it, still represents one of the most vital assets of large business, and an untapped cost-saving potential for most smaller businesses in the US. Newer communication models, like ebXML, are attempting to move away from the “message-centric” approach used by EDI to one that considers and automates the entire “collaboration” between business partners. While it seems inevitable that one of the XML “e-Business” protocols will eventually prevail, EDI is still considered to be the most practical means of transporting large volumes of transaction information.

The passage of HIPAA has effectively extended EDI’s “lease on life” by making it a requirement for the US healthcare industry. Approximately half of the present medical health claim volume is accomplished via EDI, thus making mandatory EDI a reasonable starting point for simplifying the administration of the industry. In the pharmacy industry the payment of claims is predominantly online, real-time EDI, connecting pharmacies, clearinghouses, and payers. Virtually all of the present medical EDI message traffic, however, is exchanged among a relatively small number of highly sophisticated partners: Clearinghouses and the largest payers. Our challenge now is to leverage our 50+ years of experience with EDI to extend its economic advantages to literally hundreds of thousands of Healthcare participants who have never done this before.

We are advocating no changes to the existing ASC X12 standards involving the ISA or GS segments. It's impractical that any data maintenance requests (other than qualifier code changes) could move through the X12 and DSMO processes in time for it to be useful to the HIPAA community for Identification and Routing.

The Problems

We want to define a neutral, efficient technology based on standards to be used for the routing of standard EDI transactions in Healthcare. A major hurdle to EDI is finding out how to exchange EDI transactions with one's partners without burdensome and manual processes. Manual EDI enrollment processes are a significant barrier to Healthcare administration, and an open standard based Registry of electronic partner profiles is a technical solution worth investigating.

This effort looks at the EDI interchange - substantially above the business data - and deals with message addressing and various transport methods that may be supported by willing trading partners.

Some questions which motivate this project:

(1) How would a provider know where to even send a standard transaction to whatever entity handles them on behalf of the plan or payer?
(2) A payer might have multiple "portals" for different types of transactions (say, "real-time" vs. batch) - how does he convey that to any provider who might want to send standard transactions?

(3) How does a payer know whether a provider even supports EDI in the first place?
(4) Assuming a provider supports EDI, how would a payer know that particular provider supports particular transactions (e.g, an 835 EOB - there's nothing in the 837 which says 835s are expected in return).
(5) Where would the payer send the transactions?
(6) How would a payer or provider tell trading partners the communication protocols he supports? If he's using some of dial-up system, how does he convey logon IDs and passwords? Where does his X.509 Digital ID public key reside?
(7) How does a payer say what his requirements are for ISA and GS fields?
(8) How can he tell the provider that he can't handle more than 5000 claims in an individual 837?
(9) How does someone report errors beyond the standard TA1 and 997? Does he support the 824? Or e-mail? - if so, what e-mail address should be used for sending error messages?

We can substitute " agent" (such as a Clearinghouse, re-pricer or Third Party Administrator) for "provider" or "payer" above: it just changes who has to "worry" about identification and routing.

Any of these problems can be solved the old fashioned way: through telephone calls, e-mail and paper Trading Partner Agreements (TPAs). They can sometimes be delegated to one's Clearinghouse. If we agree that paper TPAs, paper "Companion" documents and lots of e-mail and phone tag are undesirable, we might ask if any or all of these problems can be solved in an automated fashion. Or - along the road to complete automation of EDI enrollment - can this information be advertised somehow so partners know where to look? Can it be expressed in a mechanical fashion for consistency and rudimentary automation?

Our proposed solution - which entails recommendations based on the open ebXML CPP (electronic Partner Profile) and Registry specifications - satisfies many of the requirements posed by these problems.

Transport

The HIPAA TCS Rule is silent when it comes to just how standard transactions are to be sent. So EDI could be sent via dial-up BBS, e-mail, bi-synch 3780, FTP, X.25, EDIINT, and so on. But, generally, if a provider wants to send direct to the payer (point-to-point), the payer dictates the protocol. Because of the multitude of various protocols, and the difficulty of finding the EDI "addresses" of trading partners, most providers will probably choose to use a Clearinghouse. It's unrealistic to restrict transport methods to the common TCP/IP protocols. We need to support all the "legacy" dial-up connection types - to assuage fears of the open Internet's security "problems" or to simply support the existing Practice Management Systems (PMS) - with some means to describe scripts, logins, passwords, modem-settings, etc. in our Electronic Partner Profile. The Electronic Partner Profile must describe all communication capabilities of a partner.

We are only concerned with the packaging, routing and securing of STANDARD (HIPAA X12 and NCPDP) transactions between any two entities. We are not looking at situations where practice management software is generating or receiving proprietary formats through a

Clearinghouse; proprietary links (those not using standard transactions) to a Clearinghouse or business associate are out of scope.

EbXML

Of the various specifications coming out of OASIS ebXML, those for the Collaboration Protocol Profile (CPP) and the Registry are the most relevant to our work in WEDI/SNIP. All of the ebXML specifications are publicly available in electronic form at no cost to interested parties.

It's expected that our Healthcare electronic trading partner profiles will be adjuncts to the XML-based CPP. A CPP defines a business partner's technical capabilities to engage in electronic business collaborations with other partners by exchanging electronic messages.

We will need a means of electronically "discovering" a Trading Partner's CPP, and that implies a registry of some sort. A registry would give us something we never had before - an automated means of finding a partner's profile - and make what had been done manually now automatic, all without upsetting already in-place systems.

Identifiers

In the WEDI/SNIP ID & Routing group, we're merely concerned with the manner in which entities are identified in the ISA interchange header (and perhaps the GS) segment for routing. Our focus on the 'functional use' of the identifier in the ISA as the key to discovering the detailed EDI addressing information needed for the routing and transport of transactions. Problems caused by lack of standard identifiers (especially for providers in the absence of the National Provider ID) in the application transaction sets are out of scope for this project.

RosettaNet and other e-business initiatives have chosen to identify every partner using the same ID domain, such as DUNS. This is effective in supply chain, where the DUNS identifier domain has universal coverage of business entities.

In healthcare, it is impossible to force all players to identify themselves using IDs from the same domain. Providers may prefer to always identify themselves with Federal Tax ID (TIN) - and it's then incumbent then for all his partners (e.g., payers) to address the provider with her TIN in the ISA. Another provider, like a hospital, may choose to use its HIN (Health Industry Number) for procurement transactions, but the DUNS when exchanging administrative HIPAA standard transactions with payers. Finally, insurance companies may choose to be identified with their NAIC Company codes.

Most entities have at least one ID from multiple domains - e.g., incorporated providers most certainly have both a DUNS and a TIN. A commercial insurance carrier has not only a DUNS and a TIN, but also a NAIC Company code. Some companies even have more than one ID from the same domain - it's easy to have multiple DUNS numbers due to mergers or acquisitions. The Federal Tax ID number doesn't have the same weaknesses as the Social Security Number

(SSN) used for individuals - it's almost never used for authentication, but only for identification. Even so, some incorporated entities may still prefer not to use it to identify itself with the TIN, favoring the DUNS instead.

An exchange of HIPAA standard transactions is generally initiated by the provider, e.g., sending a claim. It's often easy enough for the provider to obtain the payer's EDI ID; for example, the NAIC Company code of the payer could appear directly on the patient's insurance card as the "electronic" EDI ID for inquiries and claims. The NAIC Company Code identifier can then be used to locate the payer's CPP in the Registry.

How does the payer know where to address the provider it's responding to? There is no clear means in the 837 or 270 transactions for the provider to tell the payer which ID and domain to use for addressing response transactions. A convention to always use the TIN for ISA IDs might solve this problem, but forcing an inflexible naming system on all partners is undesirable.

The use of standard identifier domains (e.g., the TIN or DUNS) to identify parties (e.g., providers, payers, re-pricers, Third Party Administrators, Clearinghouses) on the ISA is far preferable to the current practice of payer-assigned provider IDs. Not only providers, but payers, too, find it cumbersome to deal with proprietary payer-assigned IDs as EDI Identifiers on the ISA. Entities know their own standard IDs. A payer would rarely have to ask Dun & Bradstreet for the DUNS of her trading partner; more often is the case your trading partner would give you his DUNS - telling you that's how he is addressed in the ISA.

Standard Identifier Examples

Some examples follow, with the punctuation typically used to make the printed ID more readable. Dashes in the DUNS and the FEIN (TIN) would not be present in EDI data or the keys into the Healthcare CPP registry.

DUNS:

04-643-0013 - CHILDREN'S HOSPITAL, COLUMBUS , OH
07-164-3589 - RIVERSIDE METHODIST HOSPITAL,COLUMBUS , OH

Federal Tax IDs (FEINS):

23-2229683 - Aetna Inc.
61-0647538 - HUMANA INC.
95-4505291 - UCLA Orthopaedic Surgery Medical Group

NAIC:

68241 - Prudential
60054 - Aetna
54771 - Highmark

HCFA Carrier (Medicare)

16360 - Nationwide - Ohio
00880 - SOUTH CAROLINA BC/BS

HIN (Health Industry Number):

410900E00 - RIVERSIDE METHODIST HOSPITAL, COLUMBUS,OH
410810E00 - CHILDRENS HOSPITAL, COLUMBUS,OH
432740K00 - ST THERESE MEDICAL CENTER, WAUKEGAN,IL

ABA Routing Codes for Banks:

071000013 - BANK ONE, NA, CHICAGO
021000018 - The Bank Of New York

We are attempting to develop recommendations to the Healthcare industry for Trading partner identification and transaction routing. In order to fulfill the spirit of the HIPAA law, it must be possible for entities willing to use the standard transactions to have a somewhat predictable and standardized means of getting their standard transactions to payers.

IDs can't be used for authentication: there's nothing secret about them. You can easily find a company's DUNS, even if it didn't give it to you. And one can easily find out what an insurance company's NAIC Company code is, even if the payer doesn't give it out. Likewise with HINs and eventually, National Payer and Plan IDs. Since IDs are easy to discover (even lacking a central database), they make ideal EDI IDs - but lousy passwords! Even so, "discovering" a payer's ID should be simple- the provider should be able to find it on the back of the patient's insurance card.

X12 ISA Supported Identifier Domains

01 - Duns (Dun & Bradstreet)
14 - Duns Plus Suffix
20 - Health Industry Number (HIN)
27 - Carrier Identification Number as assigned by Health Care Financing Administration (HCFA)
28 - Fiscal Intermediary Identification Number as assigned by Health Care Financing Administration (HCFA)
29 - Medicare Provider and Supplier Identification Number as assigned by Health Care Financing Administration (HCFA)
30 - U.S. Federal Tax Identification Number
33 - National Association of Insurance Commissioners Company Code (NAIC)

ZZ - Mutually Defined

Proprietary IDs

Today, it's common for each healthcare clearinghouse to maintain a list of payer IDs. The clearinghouse sometimes designates these identifiers. Other times they are assigned by the clearinghouse's trading partner or by the payer. The Clearinghouse often mandates that these codes be used in the ISA sender and receiver fields.

Routing is made easier if the payer tells everyone what its own name or ID is, constrained only by the allowable qualifiers in the ISA Interchange ID Qualifier. In the absence of the National Plan ID, we might allow for a payer being identified whatever ID it prefers - one insurance carrier might prefer the DUNS and another the NAIC. Some payers might have two or more DUNS, any of which may be acceptable to them. Likewise, some providers will identify themselves by the HIN, others by the FEIN.

But it does no service to interoperability if a provider, using HIPAA standard transactions, has to make a determination of receiver IDs depending on the particular clearinghouse used as a conduit. We need consistent and standard ways to identify all participants, including payers, Clearinghouses, Third Party Administrators, Re-pricers and Providers, in order to access CPPs in a Registry.

In order to level the playing field, providers should be addressed by their own "name," rather than forcing providers to "memorize" a bunch of payer or clearinghouse-assigned proprietary IDs for use in the ISA.

Application Identifiers

This project is not concerned with the details of using identifiers for providers, payers and contracts within HIPAA application transaction sets. Identifiers are of interest to us here in the WEDI/SNIP ID & Routing project only insofar as they are used to assist in the routing of standard transactions - i.e., when they're used in the ISA receiver field or to lookup CPP Electronic Partner Profiles in the Registry.

Sometimes, applications will have to derive an ISA receiver ID from any of the various combinations of IDs used today within the application transaction set. For example, to do routing, a payer might need some way to find the provider's DUNS, HIN or EIN - one of the ID domains allowed by the HIPAA implementation guides (IGs) in the ISA.

The Loop 1000A (Submitter Name) and 1000B (Receiver Name) "audit trail" in the 837 are unreliable means of determining the sender's EDI ID to be used for routing response transactions. Besides, the other transactions (like the 270/271, 276/277 and 835) don't have an analog of this "audit trail."

The ISA is incapable of carrying application data, and the ISA sender and receiver IDs must be

valid identifiers from a limited set of domains, e.g., HIBCC HIN, NAIC Company Code, Dun & Bradstreet DUNS, IRS Tax ID (FEIN), etc. IDs of this sort can serve as both routing identifiers and application identifiers. Therefore, it's entirely possible that any of these also appear in the application NM1s (e.g., the 837's 2000A loop to identify the billing provider). One of the NM1 application identifiers (say, the Tax ID) for identifying a provider could be used to locate the provider's CPP (Electronic Partner Profile). The CPP would then tell the payer what identifier to use in the ISA for the receiving provider. It would be mere serendipity if it turned out to be the same (the Tax ID in this case) - it could just as well be the DUNS or HIN of the provider.

Depending on attributes of the desired exchange (e.g., functional group of the response, say the 277), the CPP may provide a DeliveryChannel ("EDI Address") describing the portal to which the interchange is sent, along with the desired receiver ID to be inserted into the ISA. This ISA receiver ID may very well be different from that of the sender ID on the interchange containing the original 837.

Imagine the scenario where a physician first encounters a patient. Let's assume insurance cards containing National Plan IDs come to fruition: the National Plan ID could be used to search the "National Plan ID database" to come up with the NAIC company code of the payer. From there, the Healthcare CPP Registry would be searched on the NAIC to come up with the CPP (Electronic Trading Partner Profile) to say how to deliver eligibility inquiries and claims to the payer handling the particular plan. Until the advent of the National Plan ID, the NAIC company code of the payer could appear directly on the insurance card as the "electronic" EDI ID for inquiries and claims.

Unfortunately, there's no way for the provider to use the 270 Loop 2100B (Information Receiver Name) to convey his DUNS to the payer for use in returning the 271 Eligibility Response. If the provider chose to identify himself by DUNS, how would the payer know which ID to use in the response's ISA? We need a means for the payer to auto-discover the "return path" back to the provider.

The provider's sender ID in the ISA is used only for TA1 and 997 acknowledgements. There must be some other means of figuring out the ID of the provider for application responses. The ISA sender ID is long gone, discarded by the translator, by the time the response is translated. It is best that the receiver ID be derived from the application data (or other data known to the payer) - rather than saving the ISA sender ID. This may not be a problem for the payer in the case of in-network providers (where the payer would have the provider's "preferred" EDI ID - e.g., the DUNS - on file). But a non-participating (out-of-network) provider has to have some means in the 270 transaction to give the payer his preferred EDI ID - or at least an ID that can be used to find his CPP containing his preferred EDI ID.

The 837 Claim seems to have gone halfway in acknowledging this problem, and provides a way for the provider (or his agent) to send the "Electronic Transmitter Identification Number" (ETIN) to the payer in the 1000A Submitter Name loop. But there's no way to say whether that code is a DUNS, a Tax ID, or a HIN, or whatever - the 837 IG un-helpfully says "Established by trading partner agreement." Like the 270, the 837 does have a way for the provider of telling the payer his FEIN (Tax ID) in the 2010AB Pay-to Provider loop. But the FEIN may not necessarily be the provider's routing ID used in the ISA receiver field.

Interchange Envelopes

There are only a few ways entities can be identified in the ISA based on the constraints HIPAA imposes on the ISA Interchange ID Qualifier. For providers, generally only the DUNS (and DUNS with suffix), the Federal Tax ID (or FEIN), or the HIN are acceptable domains for identifiers - assuming we rule out the 'ZZ' (Mutually Defined) qualifier. The ZZ qualifier is usually used for payer-assigned provider IDs, which are the bane of standardized identification. It is assumed that once the National Provider ID (NPI) is in place, it will be added as one of the acceptable ID types in the ISA.

X12 is meant to be independent of the transport method. The ISA only needs to hold "logical" identifiers that represent the sending and receiving entities - and 15 characters is more than enough for any conceivable identifier (e.g., DUNS, FEIN, HIN, NAIC, or even the National Plan ID and National Provider ID).

It was always understood that some sort of mapping table (whether at the VAN or Clearinghouse, or even within EDIINT software) would take a logical identifier and "map" it onto an "EDI Address." An EDI Address would be a particular mailbox (in the context of a VAN or Clearinghouse), or the protocol and addressing specifications in the case of EDIINT or FTP. Our project takes EDI Addresses to an extra level of indirection: identifiers would be "mapped" to a CPP, which in turn contains one or more EDI Addresses (selected by preference or functional purpose, e.g., "real-time" vs. batch). Each "EDI Address" would describe "where" (physical address, e.g., FTP address) and "how" (packaging, e.g, X12.58 security or EDIINT) to send the interchange.

The logical identifiers used in the ISA are fairly static - the DUNS, FEIN (or even an NPI, if it comes to pass) don't often change for the same entity. But EDI Addresses are ephemeral, subject to the whim of the recipient: one day a payer may want claims to go directly to her via FTP, and the next day she might change her mind and have them go through a Clearinghouse. A dynamic mapping system keyed on logical identifiers accommodates this nicely.

The ISA08 receiver field is not an "EDI Address," but rather it's the recipient's EDI Identifier. An "EDI Address" is all the technical information defining the protocols, port addresses and other desiderata for moving EDI data to a particular point (e.g., FTP addresses, dial-up telephone numbers, etc.). The EDI Identifier in ISA08 will be used to retrieve the recipient's CPP (Electronic Trading Partner Profile) from a Registry, which in turn will contain the appropriate EDI addresses.

It's possible that interchanges can go "out the door" with identical ISA08 values (identifying the receiver), but be routed to different EDI addresses because of their specific transaction payloads." For example, "real-time" 270s might be directed to a different EDI address than "batched" 837 claims.

We can accommodate the ZZ qualifier in our CPP Electronic Partner Profile. The receiver can specify in his DeliveryChannel ("EDI Address") that the ISA Receiver Interchange ID Qualifier and ID are to be whatever he deems fit. Perhaps his DeliveryChannel is assigned to his clearinghouse, and the clearinghouse only knows him by some contrived or proprietary (Clearinghouse-assigned) receiver ID using the ZZ "mutually-defined" qualifier. Since the

receiver is a customer of the clearinghouse, he knows ahead of time what his proprietary Clearinghouse-assigned receiver ID is, and can place it in the CPP so senders know what to use in the ISA receiver field.

On the other hand, the sender would have no way ahead of time of knowing what proprietary ID to use in the ISA receiver field until she accessed the receiver's CPP. No proprietary IDs can be used to search the Healthcare CPP Registry since there would be no way to ensure their uniqueness across all CPPs for all entities. That same ambiguity doesn't exist for Registration Authority (RA) centrally managed identifier domains, e.g., HIBCC HIN, NAIC Company Code, Dun & Bradstreet DUNS, IRS Tax ID (FEIN), etc. NAIC Company Code 54771 is uniquely Highmark's.

A sender should not be compelled to identify herself with a proprietary ID. Given the Open-EDI aspect of HIPAA, a payer may not even know ahead of time that he's about to receive a transaction from some provider: he would not have any way of assigning a proprietary payer-assigned ID to her. On the other hand, if she chooses, a sender may identify herself in the ISA sender field with a ZZ qualified sender ID - in actuality, she may have been forced to by her own VAN or clearinghouse.

It doesn't matter that the sender ID is a ZZ-type mutually defined identifier: the receiver never uses the proprietary ID except when turning around the TA1 or 997. If an interchange using a ZZ-qualified sender field were being acknowledged, then the TA1 and 997 would have to be returned to the same clearinghouse the original interchange arrived from, simply because only that clearinghouse is guaranteed to know how to interpret the ZZ (mutually defined) ID.

In order to determine the receiver ID of application responses, the sender would use one of the NM1 "application" identifiers (e,g, , the Tax ID) to locate his partner's CPP, which in turn (using the DeliveryChannel) says how to get the response where it's going and what to place in the ISA receiver field. Once the CPP was found of the receiver, the EDI Address might say to the sender that the ISA receiver field is to be a ZZ-qualified proprietary ID which has a meaning only in the context of a particular payer or Clearinghouse.

Application Intermediaries

All parties, not only the "end destination" providers and payers, can be identified on the ISA for routing of standard transactions. If an 837 is to go to a particular repricer, you're probably going to have to explicitly put the repricer's identifier (perhaps a DUNS or an EIN) in the ISA receiver field. And, likewise, if you want a 270 to end up at a particular Third Party Administrator, that TPA's identifier will have to appear in the ISA receiver field.

See "EDI Meets the Internet: Frequently Asked Questions about Electronic Data Interchange (EDI) on the Internet," RFC 1865 at http://www.ietf.org/rfc/rfc1865.txt, especially sections 5.8. It asks *Can the ISA 06 or 08 identify any entity other than the 'end' Trading Partners (i.e. a routing entity)?* Also see 5.10: *Are there other options for routing EDI X12 messages?*

...although the ISA06 and ISA08 elements are supposed to be used to identify the sender and

> receiver of the interchange, the receiver of the interchange could be a clearinghouse (as well as a VAN) that processes the interchange and then forwards the data to the ultimate recipient. In this case, you could put the receiver ID of the clearinghouse into the ISA08. The clearinghouse would probably have to determine the ultimate recipient of the message by looking inside the transaction set (or perhaps by using the GS03).

Though this IETF RFC is obviously not a HIPAA document, it proves as of 1996 that addressing intermediaries was not an unacceptable practice. The TA1 and 997 go back to the sender in the ISA, whether a clearinghouse, billing service or the "real" provider.

The Present Situation

The present environment within Healthcare for routing of transactions is payer-centric. It could keep going that way, but the future health care electronic traffic will include provider-to-provider transactions involving delivery-of-care. Having every provider set up in advance with every possible other provider is not very practical. In the future, eventually, providers will participate, not as clients, but as equal participants. Especially, a sender will be able to send an asynchronous message and the provider will be able to receive it. This is a hugely significant change from the payer-centric mailbox model now used for batch transactions and the client/server model now used for DDE transactions

The dominant business model in health care today is:

1. For the most part, only health care claims are submitted electronically by providers to the party they've determined is financially responsible for reimbursement.

2. The format used for electronic claims is most often the NSF batch file format, or some variant thereof.

3. It's not typical that a provider submits claims directly to the financially responsible party. Rather, intermediaries are more likely than not to be in the picture. Intermediaries can be clearinghouses, TPAs, repricers, billing services, and so on.

4. These intermediaries typically determine the financially responsible party by interrogating data contained with the batch file.

5. While the NSF batch file has batch header and trailer records which start/end the batch, the records in the batch are fixed field/fixed record multiple record types.

6. The industry does not use the typical EDI VAN store and forward model. Thus, it has not built an infrastructure that uses an identifier from a batch header record to "mailbox" files for the receiver.

7. The industry model is one of the provider always have to "push" electronic claims to the financially responsible party through an intermediary and to then "pull" any return messages.

8. Other types of information exchanges, queries, referral requests, etc, are most often

performed via phone, IVR, DDE, or fax. Thus, today's application systems do not typically support nor enable batch file transfers for these types of information exchanges.

The model most other industries use for standards-based EDI exchanges is one where the receiver of the interchange maintains a mailbox at some "post office" - most often called a VAN or Value-Added Network. Thus, both parties to the information exchange maintain their own mailboxes (or multiple mailboxes) at a post office(s) of their choosing. It's this model that the current X12 control structures enable and support quite adequately.

The Functional Group

In the supply chain sector, the common practice has been to use the same values at both the ISA and GS levels, unless the sender and receiver have agreed to use the GS identifiers to identify, for example, a business unit or operating unit within a larger enterprise.

For HIPAA healthcare administration, we can envision a payer specifying GS receiver code(s) for one or more adjudication systems and yet other GS receiver codes for other types of transactions. This is closer to the original intent of the GS application identifiers. When this approach is used in Healthcare, a capable EDI translator can then output the correct file to the correct backend adjudication system.

The HIPAA implementation guides haven't provided explicit guidance for the use of the ISA/GS identifiers, nor for the standard acknowledgments, such as the TA1 and the 997. The GS segment contains not a Sender ID or a Receiver ID, but rather an Application Sender's Code and an Application Receiver's Code. They are intended to for use in internal routing and translation map identification. In some cases, this GS information is needed to determine which application gets the translated data.

Generally, the GS elements cannot be standardized, though the 270/271 implementation guide makes some recommendations on how to distinguish between Batch and Real Time transactions using the GS receiver application code:

> If trading partners are going to engage in both real time and batch eligibility, it is recommended that they identify the method they are using. One suggested way of identifying this is by using different identifiers for real time and batch in GS02 (Application Sender's Code) for the 270 transaction. A second suggested way is to add an extra letter to the identifier in GS02 (Application Sender's Code) for the 270 transaction, such as "B" for batch and "R" for real time. Regardless of the methodology used, this will avoid the problems associated with batch eligibility transactions getting into a real time processing environment and vice versa.

Overloading the GS sender code (used solely for internal routing by the recipient) is certainly preferable to requiring different sender or receiver IDs in the ISA, depending on whether Batch or real-time processing is desired.

Clearinghouse Aggregation

It's important to emphasize that for any one X12 interchange, there's only one sender (or submitter) and one receiver - regardless of the number of providers whose "claims" are embedded in a single 837. The sender is the entity that creates the ISA. The receiver is the entity that returns the TA1 and/or 997(s).

Interchange routing is only concerned with the identification of the trading partners (who may be clearinghouses, billing services, re-pricers, etc. - not just providers or payers) at the ISA level, and the issues of transport. This is the minimum necessary to be known in order get the interchange from here to there.

What any intermediary, such as a clearinghouse, does with the enclosed transactions (and functional groups) is beyond the scope of this project.

Clearinghouse aggregation is fully supported by the CPP EDI Address function. For example, consider the situation of a sophisticated provider, such as a large hospital chain, which wants to send standard claim transactions to 20 payers. The hospital can look these payers up in the Healthcare CPP Registry; perhaps it finds that 10 of the payers are supported by the same clearinghouse, and that claims for any of the 10 are to be directed to the same "portal" resident at the clearinghouse.

The hospital could choose to build 10 interchanges, one for each of the payers, shunting them off to the designated Clearinghouse portal one after another. The CPP for an individual payer might even specify an alternate EDI ID to be used in the ISA receiver field - i.e., the proprietary clearinghouse-assigned payer ID.

Alternatively, the CPP for the Clearinghouse (which has been referred to indirectly by the payers' CPPs) can indicate in the Delivery Channel that claims can be "aggregated," with a special Receiver ID to be used in the ISA receiver field. This could be of benefit to both the hospital and the Clearinghouse: the sending hospital now can "aggregate," or combine, the claims for all 10 payers into one standard 837. Nonetheless, it's the hospital's option to do aggregation in this case.

If aggregation is chosen, the clearinghouse can then proceed to split and merge, combining other providers' claims (for the same payer) into consolidated 837s for each of the payers. Some payers may find it to be a big advantage in having multiple providers' claims aggregated together in the same 837. In any event, there's nothing in the Healthcare CPP Registry recommendations keeping us from elegantly supporting such "requirements."

A provider may even want to send a batch of claims to <u>different</u> payers all bundled up in one 837, for subsequent re-sorting and distribution by his own clearinghouse. More likely than not, our recommendations have no effect on this practice: the provider has determined that he would rather deal with a Clearinghouse and send a single 837, and has arranged with that Clearinghouse to do the "un-bundling" and aggregation. The provider will probably not be using our recommendations because he has no need to address, nor route to, individual payers - he has devolved the responsibility on the clearinghouse for routing transactions to the appropriate

payers.

Discriminatory Barriers to Standard Transactions

Under HIPAA, payers will have to be prepared to take in standard transactions coming from even "unknown" or out-of-network providers. If a payer would have taken paper before, it can't put up barriers discriminating against the equivalent Federally mandated HIPAA standard transactions. Not only will payers have to make available an open portal for receiving electronic claims and eligibility inquiries, but they will have to make sure their translators can accommodate ISA senders they've never seen before. The absence of a trading partner agreement does not absolve the payer of her responsibility to process a standard transaction. In summary:

1. It is potentially possible for a payer to receive an electronic claim from a non-participating provider
2. The payer cannot refuse to receive the claim
3. The payer is not obligated to process/adjudicate the claim
4. The payer should anticipate the potential for receiving electronic claims from unknown providers and have a procedure for dealing with them
5. This process would be no different than what happens today if a payer receives a paper claim from an out-of-network provider.

Mis-routing of out-of-network claims can be minimized with the implementation of the Healthcare CPP Registry. If the provider has the plan's identifier, it will obtain the correct CPP, which in turn points to the plan's open portal.

Open Portals

A payer has to process every claim received. But there is the potential to receive a claim from an unknown (out-of-network) provider, and the payer cannot reject it out of hand. The payer must at least take the claim in through its electronic "mailroom" and then decide what to do with it - the very same process a payer would go through with a paper claim that came in through the mailroom from the U.S. Postal Service. The HIPAA TCS Rule requires that payers maintain open portals for accepting standard transactions on a non-discriminatory basis.

An analogy can be made to a company's e-mail server serving as an "open portal." One never knows what's going to come across. Likewise, a payer can simply read a purported claim file coming in on the open EDI portal. Once the start of an EDI interchange is received, if the remainder doesn't conform to X12 syntax, a negative TA1 or 997 can be returned. If it looks like good EDI, but doesn't comply with the HIPAA IG, an 824 can be returned.

If a correctly formatted 837 got past this gauntlet, perhaps it's from an "unknown" provider. For payers still suspicious of EDI from unknown providers, there's always the option of taking the 837 and printing it out on a HCFA 1500 or UB92 claim form, pretending as if it came in the mail

or on the fax. At that point, the payer is home free: there's now no danger of "disadvantaging" standard transactions vis-à-vis paper. Clearinghouses do this all the time: they take in standard transactions and "drop" them to paper for the payer. Open portals are not a matter of blind trust. A payer merely has to accept a file purported to be a standard transaction from any source (which could be a Business Associate or Clearinghouse acting on behalf of a provider); he would still presumably go through the same processes he would with a paper claim.

Encryption is required by the HIPAA Security Rule when exchanging EDI data over the Internet. Key exchange is not necessary before a signed and encrypted file is read. The file is encrypted with the payer's public key, which it has freely made available to partners via the CPP Electronic Trading Partner Profile. The payer uses its own private key to decrypt the file. The payer can authenticate the source of the file by checking the signature against the public key supplied in an X.509 certificate pointed to by the purported provider's CPP. There is no exchange of keys: payers are expected to use and support standard ITU X.509 certificates. It may be unreasonable to expect providers to use PGP whose PKI necessarily depends on out-of-band exchange of certificates for applying trusted signatures; PGP will be unsuitable for all but the most insular trading communities.

Clearinghouses and VANs

The open-portal concept certainly does not exclude VANs from participating in Healthcare. VANs have setup considerations for their own customers, as do Healthcare clearinghouses. Generally, a provider needs the services of only one switch, assuming its own can interconnect with other intermediaries and switches. Nothing in our Healthcare CPP Registry model keeps a provider from sending all of its standard transactions through its own VAN (or clearinghouse), who in turn uses the Healthcare CPP Registry to figure out how to send interchanges to "unknown" payers' open-portals. Likewise, a Healthcare entity may host its "open-portal" at a VAN or clearinghouse, and its CPP's EDI Address would simply reflect the address of the intermediary.

There is an erroneous notion that HIPAA is a way to eliminate the need for clearinghouses, where all EDI data can go point-to-point between partners. VANs and Clearinghouses can use the same CPP Registry functionality that point-to-point software would take advantage of. The business decision concerning whether a trading partner uses a VAN or Clearinghouse, or goes point-to-point with its partners using FTP or EDIINT software, will in large part be made on price, availability, and ease-of-use. There are additional considerations, especially other VAN or Clearinghouse value-added services such as translation and aggregation.

Intermediaries, such as VANs and clearinghouses, will be able to use the CPP Registry recommendations themselves. Imagine a provider contracting with a Clearinghouse intermediary for all communications. The clearinghouse will benefit by being able to discover where the provider's partners (payers, Third Party Administrators, etc.) are automatically - and they certainly won't all be customers of the clearinghouse itself. The provider in this case has delegated the task of looking up and discovering CPPs onto the clearinghouse - which itself is a valuable service. Even so, providers who have contracted with clearinghouses for their communication services will have no direct need for our recommendations. The recommendations will be of most value for providers and payers, clearinghouses, Third Party

Administrators, re-billers and re-pricers who wish to connect to each other directly.

Trading Partner Agreements

The process of providers entering into bi-lateral trading partner agreements (TPAs) with payers can be incredibly labor intensive, drive down EDI transaction volume, drive up the cost of EDI implementation and expand the time frame to implement. From a provider perspective, if a provider chooses to contract with a clearinghouse, the clearinghouse is its trading partner and will provide a TPA defining requirements for exchanging transactions. The provider should not have to enter into a proprietary individual TPA with every payer with which it might ever need to exchange a transaction. This is of particular concern because when these proprietary agreements are required, the cost of managing the process is disproportionately assigned to the providers and their clearinghouses.

When the Federal government, most notably the Department of Defense, went full bore into EDI in the early to mid 1990's, it initially required that each supplier to the government execute an EDI trading partner agreement. This was a huge failure, and in fact became a major barrier for getting the hundreds of thousands of suppliers willing to engage in EDI with the Government. Within 6 months the Government abandoned the requirement for an EDI trading partner agreement. Other industries have also recognized the barrier an EDI trading partner agreement became when trying to establish EDI information exchanges.

With the advent of the HIPAA standard EDI transactions, Healthcare should not use a business model that clearly didn't work for other industries. A discussion of Trading Partner Agreements under HIPAA is available in the WEDI document "Trading Partner Agreements: A White Paper Describing the Business Issues and Recommended Solutions Associated with Trading Partner Agreements." It's available under "Transactions Workgroup White Papers" at the WEDI/SNIP site at http://snip.wedi.org/public/articles/Trading113000.pdf.

EDI enrolment

Today, providers who use a clearinghouse must complete three to five TPA/Enrollment forms for any of Medicare, Medicaid, BC/BS and Champus, who almost always require agreements. It takes an average of 2 - 3 weeks for a clearinghouse to receive completed paperwork from the provider and an additional 6 - 8 weeks for approval from the payer (though BCBS often approves in 2 - 3). It takes providers as long to complete their part of the enrollment paper work for these payers as it does for most to complete testing, implementation, training and full production for payers who don't require it.

Many payers are very particular when it comes to their agreements. Some require the signature of every physician in a group and most require a listing of every group number and provider ID. Some require social security numbers. Each agreement is proprietary. It often takes 2 or more attempts before the provider gets it right, making the whole process an incredible hassle.

In other situations, the payer does not require a written agreement between the provider and

payer, but does require the clearinghouse to obtain authorization. This process, while still time consuming, is far easier than executing the bilateral agreements described above.

This project wants to move the Healthcare industry toward an "electronic" TPA in place of signed paper agreements. The e-TPA or CPP Electronic Partner Profile we envision includes technical communication protocols, security and encryption requirements, and potentially even the "companion guide" type of information - all of that being generally classified as the "technical" business arrangement between the trading parties. Even if we can get all of the nuances of the "technical" business arrangement included within our electronic definition, it's unclear whether there will still be overriding legal barriers which will require each trading partner to negotiate and sign a paper document to comply with the HIPAA regulations.

We desire avoid onerous EDI enrollment procedures, negotiated TPAs, and other sundry hurdles and hoops placed in the way of providers who merely want to use the standard transaction sets. Not only are these processes exceedingly manual, but they may take months to consummate - surely impediments to frictionless e-commerce.

DeliveryChannels

Currently, the ebXML CPP DeliveryChannel does not support non-Internet transport protocols or non-ebXML packaging techniques (e.g., EDIINT). This project will look into cataloging the various permutations of media and protocols. All these criteria will be mechanically represented in some extension of the CPP DeliveryChannel structure.

A basic universal transport technique will surely include simple e-mail using S/MIME attachments. It's bi-directional, and everyone can use it today - at least as long as they're using standard e-mail clients like Outlook, Outlook Express or Netscape Communicator. For encryption and authentication, both standard ITU X.509 and PGP certificates will be supported. Compression can be provided by zipping the EDI before encryption, too. This minimalist approach accommodates everyone from the small provider to the big payer.

Additionally, EDIINT should be included, both the AS1 (SMTP e-mail) and AS2 (HTTP) varieties. EDIINT software is generally available and affordable. FTP is an option, though the small provider will often not have his own FTP server: he may have to poll drop-boxes at the payer if he insists on using FTP on the receive side. Coming of age is ebXML Messaging Services, with software vendors now providing ebXML messaging service handlers (MSH). The ebXML Messaging Specifications provide for a SOAP based packaging of business payloads for direct point-to-point transfer over the Internet - one of many packaging techniques that will have to be supported in the WEDI/SNIP ID & Routing Specifications. It will hold X12 EDI payloads, just as EDIINT does. We can expect Healthcare Clearinghouses to continue supporting the more prosaic forms of point-to-point transmissions (e.g., FTP, Kermit) which will predominate in the short term; our "EDI Addresses" must support these "legacy" transport channels.

The Healthcare Registry

Entities are always merging and acquiring - and our registry and Electronic Partner Profiles (CPP) can easily accommodate these eventualities. Any obsolete ID can still be searched on to either (1) produce a dummy CPP which in turn points to the surviving entity's CPP, or (2) retrieve the surviving entity's CPP directly (which contains the obsolete ID as a non-preferred search key).

The OASIS ebXML Registry allows us to store "pointers" to participants' CPPs, which reside as XML files in their own servers. A CPP is retrievable by one or more entity IDs. For example, a large payer may choose to be identified by their NAIC Company code. Providers, on the other hand, like hospitals, may prefer to name themselves by any of a HIN, a DUNS or a Federal Tax ID. Likewise, a small practice may be identified solely by Tax ID, at least until the National Provider ID is available.

Even if a small provider doesn't use standard HIPAA X12 transactions itself, but rather uses a Clearinghouse or Billing service as an intermediary, it would still have an entry in the Registry with a vestigial CPP which points to its respective agent (e.g., via the ID of the clearinghouse or billing agent).

When the National Plan ID does come into play, we would have multiple levels of indirection in any retrieval via the CPP Registry. Implementing search by Plan ID to arrive at the payer's CPP will be supported by indirection: the plan ID would be used to retrieve a pointer to the payer or Third Party Administrator (TPA), which in turn would be used to access that entity's CPP for technical trading partner information. Partners using the Registry will be authenticated using X.509 certificates.

Partners advertise their capabilities in their CPPs. For example, a provider would indicate in the CPP electronic partner profile that she's willing and able to take 835 electronic Remittance Advices. It could also have a notation that said she was willing to take electronic funds transfer at her bank, specifying an ABA routing code and her account number. Of course, the payer using this information isn’t compelled to do EFT, even if he does support the 835 ERA.

The registry is a federated database, built to standard ebXML specifications, and able to be accessed with a standard query protocol. Its purpose is to link the all the possible identifiers used by a single trading partner with its single CPP.