



**Payments and Patient Finance: Where the
Revenue Cycle Meets the Banking System
White Paper**

**A Work Product of the HIMSS Financial Banking and
Healthcare Task Force**

Table of Contents

Executive Summary	3
Introduction to the Banking System and Payment Networks	3
NACHA, the Federal Reserve, Financial Institutions, and the Processing of Web-Enabled Payments for Clearing and Settlement.....	6
Institutional Revenue Cycle – Processor/Bank Services	7
Introduction to the Revenue Cycle	7
<i>Institutional Provider Steps in the Revenue Cycle</i>	7
Claim Processing Today	14
<i>Claims Submission—Role of the Claims Clearinghouse</i>	15
Integrating Banking Transactions	17
The Re-association Challenge.....	17
Patient/Retail Lockbox.....	19
Insurance/Wholesale Lockbox Using Intelligent Optical Character Recognition (IOCR)	21
Online Bill Presentation and ePayment Systems	22
Consumer Driven Health Plans.....	22
Future Predictions	23
Future Considerations as Financial Institutions Conduct Web-enabled Payments	23
Payment Challenges for Financial Institutions	24
Identity Management and the Use of “Credentials”	24
Key Areas with Anticipated Change and Advancement in the Future	25
Technology Advances.....	25
Payor/Provider Systems	26
Payors.....	26
Regulatory Compliance	26
Networks.....	26
Terminals/Products	26
Consumers.....	26
Frequently Asked Questions	27
Table A: Revenue Cycle Diagram for an Institutional Provider	28
Table B: HIPAA Standard Transaction and Code Sets.....	29
Glossary of Terms.....	30
Credits.....	34

Executive Summary

Over the past several years, healthcare providers have been increasingly subjected to fiscal pressures on their margins. These issues include declining or stagnant reimbursement from payors including Medicare, higher deductibles, elevated levels of bad debt and continued complexities regarding coding, billing, collections and follow-up activities. One issue impacting the industry is the changing role that financial institutions are playing with healthcare providers. Historically, there have been long-standing relationships between financial institutions and healthcare providers. These relationships have primarily focused on the services that financial institutions offered to healthcare providers around payment clearing and settlement. While financial institutions are still offering these services to healthcare providers, there is an emerging focus by financial institutions to take on an expanded role in the revenue cycle process to address inefficiencies that exist through Web-enabled electronic transactions over the Internet.

This new convergence between healthcare organizations and the banking industry is poised to offer a private, secure digital platform that will reshape the revenue cycle process and, ultimately, the care management process. In order to accomplish this, a number of issues must be addressed including ensuring compliance with existing financial regulations, offering a higher level of security management, adopting and clarifying HIPAA transactions and providing technology upgrades by payors and providers' IT systems.

The purpose of this paper is to:

- 1) Facilitate awareness and education about the banking system and payment networks within the healthcare provider community.
- 2) Identify touch points where healthcare providers may leverage the utilization of these payment networks.
- 3) Review the intersection points with the advent of consumer-driven healthcare.
- 4) Describe where banking products may be utilized more effectively today and in the future.

Nothing in this white paper should be construed to represent that HIMSS or this task force is warranting the success of any particular entity and should not be used as a comprehensive guide of innovated banking services. The scope of this paper includes an introduction to the banking system and payment networks; an overview of the healthcare revenue cycle process including the current state of claims processing; highlights of some of the financial and banking solutions offered to healthcare providers; and future predictions. A set of frequently ask questions a healthcare provider may have on this topic is also included.

Introduction to the Banking System and Payment Networks

Financial institutions have many roles as providers of credit and operating services in healthcare. Payments to healthcare providers are a combination of “claim payments” made by health plans and other institutions reimbursing the provider and “consumer

payments” made by patients and guarantors for the patient liability portion of a reimbursement to a provider.

Those who have not had a course in money and banking may find some of the following a bit confusing. “Money” can be measured in many ways by the economists (M1, M2 etc.) but for purposes of this paper, money or “value” consists of deposits in banks, which are bank liabilities to their customers to honor checks or provide cash as requested. Payment networks process the transfers of bank liabilities from the bank of the consumer or health plan to the bank of the provider, which are the reimbursement for healthcare services provided. With the understanding that money consists largely of bank deposits, or bank liabilities, how do the banks enable payment?

Every bank in the United States is a member of the Federal Reserve System of 13 Federal Reserve Banks and every bank has an account at the Federal Reserve. Banks often settle financial obligations amongst themselves by moving funds from one bank’s account at the Federal Reserve to another bank’s account at the Federal Reserve. Banks “clear” payment transaction amongst each other and often “settle” their inter-bank obligations by moving funds among their accounts at the Federal Reserve Bank. The underlying transactions do not directly involve Federal Reserve settlement and are best understood by describing the options that are used at the provider site.

Payments to a provider can be made by cash, check, electronic funds transfers and credit and debit cards. Providers work with their banks to have the right “treasury” or “cash management” services in place to accept these payments and manage the related accounting. Cash is usually the least used payment method. It requires safekeeping and protection, making it the most expensive payment to process. Checks are commonplace yet labor intensive for providers to accept. Unlike cash that must be counted at the bank by a teller, each check has data stored on the bottom to allow for processing partly by machine. Also, each check is printed with a series of magnetic ink characters on the bottom, which are supplemented by the depository bank and then routed to the issuing bank for payment. Mind boggling as it may sound, the banking system routes billions of checks among the various banks to complete payments. Local “clearinghouses” have exchanged physical checks among banks for decades. Net settlements based upon the total dollar amount of checks processed are “settled” among the banks daily, often by moving money from one bank’s Federal account to another bank’s Federal account. These settlements between banks are transparent to the users of checks except for those providers who closely examine a bank’s “availability schedule,” indicating the time check deposits are made available for investment.

Electronic funds transfers consist of Fedwires and Automated Clearing House (ACH) transactions. Fedwires are same-day real-time funds transfers where the paying organization can ask its bank to move money from the Federal Account of the originating bank to the Federal Account of the receiving bank. These cost upwards of \$15 for both the payor and the provider and are seldom used outside of occasional Centers for Medicare and Medicaid Services’ (CMS’) payments to hospitals with a severe cash flow problem. The ACH payment system is operated on contract with the Federal Reserve

System (with a few exceptions). The ACH system operates as the primary payment system for electronic funds transfers such as payroll deposits, social security deposits and “trade payments.” Trade payments are those made to settle invoices, claims or bills submitted by commercial enterprises. Every bank in the United States that participates in the ACH must abide by rules promulgated by the National Automated Clearinghouse Association (NACHA); these rules cover file formats and bank responsibilities for participation in the network. Although many people in healthcare may discuss “wiring money,” they usually refer to ACH payments, which are more like checks than wires. ACH payments are “next day” items, like checks and are very inexpensive to originate and receive, like checks. ACH files pass between the banks via ACH clearinghouse computers in a proprietary private network. That network can carry ACH files in multiple formats governed by NACHA that are processed in a fashion similar to files created during check processing. The major difference is that ACH files can contain more information than checks including crucial trace numbers that relate to electronic remittance files sent to the payee or a full ANSI X12 remittance file. This additional information may be on a check stub or remittance advice but not on a check.

The HIPAA implementation guidelines to the electronic claim payment allow only checks and two ACH formats to support the transmission of money and data through the banking system. Providers must determine how they get their ACH information reported from their bank posted into their patient accounting systems. Providers may also utilize the ACH network to initiate repetitive payments from patients on a payment plan. Also, some providers utilize the ACH process to make electronic trade payments to suppliers, payroll and tax payments. When providers are paid electronically, payment processing costs are less than when they are paid by checks; however, the provider must obtain electronic data interchange (EDI) reporting services from his or her bank to manage the reconciliation of the bank account and the re-association with remittance data sent separately from funds. EDI bank reporting improvements can be made to support reconciliation and re-association requirements at the provider organization. As providers process payments electronically from more payors, and, as trading partners and additional payers utilize EFT, bank reporting and re-association services will grow in importance.

Providers are also increasing their utilization of consumer payments via debit and credit cards. These are sometimes called “payment networks” but the funds settlement for all credit card transactions is an ACH deposit sent to the provider by the card vendor. American Express, Discover, Visa and MasterCard (vendors) may all contract with a provider. These “merchant card” relationships require that a file be transmitted by the provider. At some point afterwards, a payment is made by the vendor to the bank account of the provider via an ACH transaction. Again, the challenge to the provider is obtaining the detailed information required from the bank and from the card vendor to reconcile the payments to the submitted files and to the amounts posted to the patient accounts. These “payment networks” move data but money is moved between banks via the ACH transactions described above. Credit card and debit card transaction are priced and work somewhat differently. A debit card (which is often the instrument tied to a consumer driven health plan) utilizes the information process that governs the ATM network. An accepted debit card transaction provides a guaranteed movement of funds from the

consumer's bank account to the provider's bank account. As consumer transactions increase, healthcare providers should utilize the sophisticated banking services that support the retail industry, which will generally change the point of sale "cashiering" business processes within the provider organization.

This is a highly compressed description of the banking system and other resources should be reviewed to completely understand the details of what money is and how payments work.

NACHA, the Federal Reserve, Financial Institutions, and the Processing of Web-Enabled Payments for Clearing and Settlement

NACHA, The Electronic Payments Association announced in April 2008 that live transactions were originated using NACHA's Electronic Billing Information Delivery Services (EBIDS). A task force of financial institutions, telecom companies and high volume "billers," with the assistance of the Cleveland Federal Reserve Bank, developed an infrastructure to enable businesses and financial institutions in using the existing ACH Network. This infrastructure would use the Network as a universal, electronic channel with open standards for the distribution of consumer bills and to all financial institutions that use the ACH Network. Businesses are able to deliver electronic bills to a consumer's financial institution for presentment to the consumer in the online banking platform and to receive authorized credit payments through the secure ACH Network.

The goal of the EBIDS project is to increase the number of businesses and financial institutions that can support electronic bill presentment and payment. Since large and small financial institutions can utilize the ACH Network for presentment and payment, new markets for a richer, more diverse group of financial institutions are provided. The goal is to increase the adoption rates for e-bill presentment and payment across the board.

The model allows a business to originate a zero-dollar ACH transaction containing a summary of the consumer's bill in an addenda record. The transaction routes through the ACH Network from the business's financial institution to the consumer's financial institution and is presented to the consumer in a designed secure online session. The consumer authorizes payment without disclosing account information to the business. The consumer's financial institution originates the ACH credit with remittance information to the business's financial institution.

The EBIDS system moves electronic bill enrollments, bills and payments through the ACH Network under the existing rules and interoperability infrastructure with open XML standards for addenda information. EBIDS is transparent to the consumer and offers a number of consumer benefits such as receiving and paying bills in an identity-managed, authenticated and trusted environment within their online financial institution's site.

NACHA represents more than 11,000 member financial institutions, a network of regional payment associations, organizations and various councils who manage the development, administration and governance of the ACH. The ACH Network currently provides an efficient, reliable, and secure payments system that facilitates commerce

electronically. NACHA provides its members with the “NACHA Operating Rules” to manage the ACH Network, promotes the value of ACH payments and offers tools and resources to facilitate the adoption of ACH payments.

The review of this effort is to stimulate dialogue and increase understanding between vibrant, diverse healthcare providers and operations with the richness, security and privacy provided by the payment networks of financial institutions. This will broaden the participation of cross-industry collaboration between the public and private sectors, with the goal of reducing the cost of healthcare to consumer/patients and improving the quality of care.

Institutional Revenue Cycle – Processor/Bank Services

Introduction to the Revenue Cycle

The revenue cycle has evolved over decades to include multiple exchanges of information among providers, payors and patients. The process is complex and a uniquely American administration of reimbursement for healthcare services rendered. Each of the key information exchanges in the revenue cycle is enumerated below with commentary about payment processing and the interaction with the banking system at that point in the revenue cycle.

The revenue cycle contains the steps a patient takes when scheduling a visit to an institution (hospital) as an elective admission, clinic or outpatient visit or using the emergency room until the account is billed and any patient obligation is paid or written off. What is described is the best practice solution to automate and use the HIPAA transactions to reduce the length of the revenue cycle. Tables A and B, located at the end of this document, illustrate the revenue cycle steps and describe ANSI X12 transactions mandated by HIPAA. They also include the use of bank reporting for patient payments whose payments are not “covered transactions” under HIPAA. These may be accommodated by banking standards other than X12 transactions mandated under HIPAA.

Institutional Provider Steps in the Revenue Cycle

1. Scheduling
2. Pre-Register, Pre-Admission
3. Benefits Confirmation, Authorization
4. Financial Counseling
5. Registration, Check-In, Bed Control
6. Charge Entry, Revenue Protection
7. Care Documentation, Encoding
8. Billing, Claims Submission
9. Health Plan Payments
10. Denial Management
11. Health Plan Follow-Up
12. Secondary Billing
13. Patient and Guarantor Billing and Collections

14. Account Collections, Write-Offs

The electronic transactions below are often identified by their X12 numbers and not the full X12 name for each transaction.

1. Scheduling

Provider Process Steps

- For elective inpatient visits, schedule the admission.
- For outpatient and clinic visits, schedule the visit.

Payment Service

- None

2. Pre-Register, Pre-Admission

Provider Process Steps

- Collect the financial and demographic information on the guarantor and the patient.

Payment Service

- Process any type of patient payment—the deductible, co-insurance, co-pay or minimum deposit due from the patient based on the institution's evaluation of the patient's liability and ability to pay.
- The role of payment service is to access the payment networks. The sources of payment may include cash, check, and ACH debit initiated by the provider or acceptance of debit or credit cards. The actual funding accounts may have different tax names and tax treatment such as healthcare savings accounts or flex spending accounts but the different payment mechanisms can be used to remove funds from the same account. There are multiple technologies for payment processing at the provider site (cashiering) including onsite electronic deposit of checks, initiation of credit card or debit card transactions or creation of an electronic file that will use the ACH network to debit the patient's bank accounts.
- This service can occur at the time of admission or registration or later in the revenue cycle process.

3. Benefits Confirmation, Authorization

Provider Process Steps

- Check the patient's eligibility (270/271) and create the insurance verification (policy limits, deductibles, etc.) for the patient accounting system.
- Get authorization/referral from the Payor (278).
- Integrate eligibility and authorization/referral responses into the patient's folder in the document imaging system.

Payment Service

- None of these steps were completed during pre-registration but many patients show up at the facility with an appointment (ER treatment) and the steps above for payment may take place at the time of service.

4. Financial Counseling

Provider Process Steps

- If the patient has indicated an inability to meet the financial requirements, they can explore alternative arrangements. This can be done prior to admission, at admission, or while the patient is in the institution.

Payment Service

- Financial counselors can collect some funds at this point and arrange for a payment program that is agreed upon by the patient. This may result in payments via any of the payment mechanisms and payment sources available to the patient.

5. Registration, Check-In, Bed Control

Provider Process Steps

- Patient responsibility payment for services can be collected at time of check-in if it was not collected at pre-admission. Typically, the patient will be notified of any obligation and will present cash, check or a credit card for payment and the payment will be processed at the time of registration or admission.
- For inpatient stays, an estimated co-pay can be collected up front and can be reconciled after services are rendered.
- The accounting transaction for the money received can be either posting it electronically from a bank file of processed payments or manually processing and entering it into an online payment posting system.
- Registration documents can be filed in a patient's folder or in an electronic patient folder in a document imaging system.

Payment Service

- Providers can process any type of patient payment using the banks merchant services and the banks card device(s) to process the deductible, co-insurance, co-pay or minimum deposit due from the patient, based on the institution's evaluation of the patient's finances. If the patient has a healthcare savings account or flex spending account, the payment is deducted from the patient's bank account and the money is transferred to the provider's bank account. The bank creates a posting file with the payment information to be sent to the institution's process for posting to the patient's account.

6. Charge Entry, Revenue Protection

Provider Process Steps

- During a patient's stay, he or she will have services/procedures performed. Automated entry from clinical departmental systems provides input of charges for services to the patient's account.
- The utilization review staff validates the stay based on the payor's criteria for reimbursement.

Payment Service

- None. If any money is collected, the bank and processor would perform similar functions as described at the time of registration.

7. Care Documentation, Encoding

Provider Process Steps

- Clinical systems capture nursing notes/test results that can be used by medical records for supporting documentation (as claim attachments) when needed for certain DRGs or APGs. This is necessary for getting the claim paid on a timely basis.
- Services for medical records to maximize the coding of ICD-9-CM and CPT4 codes for groupings to maximize reimbursements.

Payment Service

- None

8. Billing, Claims Submission

Provider Process Steps

- To this point in the revenue cycle, the provider has pre-registered the patient and ideally, collected the correct information from the registration process. This means the provider has collected the necessary information for the claim, identified the patient's insurance, checked his/her ability to pay, collected a deposit, integrated the charge detail from the clinical systems and coded the procedures and diagnosis. After this work is done, the provider can submit the 837 claim to the payor.
- A claims management system may be used for the claims submission process. The function of this type of system is to check the claim data being submitted for general problems using a series of 'edits.' Once claims are accepted into the claims management systems, they are processed through another setup of checks and edits specific to the payor. This is necessary because each payor has a "Companion Guide" providing details about their use of the ANSI 837 claims submission transaction. These edit steps help to assure the claim is clear of errors and will be accepted for processing upon submission. A best practice for hospitals is to submit a 'clean' claim for processing within three days from discharge.
- Providers use contract management systems in order to calculate expected reimbursement for their managed care contracts.

- Once the claim information is completed, the business office submits a clean claim to their clearinghouse for submission or sends the claim direct (837). The goal of all hospitals is to complete the process in 3 days after discharge.

Payment Service

- No payment service at this point.

9. Health Plan Payments

Provider Process Steps

Background: For the purpose of this paper, claim payments consist of both remittance information and funds transfer. Process steps must include cash management process steps for paper and electronic payment and remittance processing steps for paper and EDI remittance data. Providers may receive health plan remittance data and checks at their facility, while other providers outsource the function to a bank. Such outsourcing utilizes a bank lockbox service where the bank handles receipt of mail and deposit of checks. Additional services may include imaging all checks and explanation of benefits (EOB) plus correspondence. In addition, some banks convert the images to EDI ERA files for automated posting. The steps below will describe mail and check processing. Providers may perform all of these functions internally so the process steps below will speak to both provider functions and bank lockbox functions for the same process steps.

- Providers receive many claim payments via paper checks, EOBs and explanation of payments (EOP) documents that are sent to their business office via the postal service or to a bank lockbox. Mail room sorting of claims payments, cashing checks, photocopying checks and creating and imaging posting batches may be done by the provider internally or outsourced to a bank lockbox operation.
- Providers must manage the deposit function for paper checks and receipt function for electronic funds transfer (EFT) payments. All payments received must be accounted for. Providers create batches for processing and reconcile the posted cash amounts to the cash received. Electronic funds transfers must be “reassociated” with electronic remittance information *before* electronic remittance advices (ERAs) are posted, a requirement of generally accepted accounting principles. Providers must obtain bank deposit reports daily and determine which credits to their accounts relate to ERAs received separately. This re-association task increases as more and more payors convert to EDI payments and separate data and dollars.
- “Cash” posting “relieves” a receivable in the patient accounting system. The accounting transactions are limited to posting a credit for the payment, recording a contractual adjustment or posting a write-off. The difficulty of the posting process is not so much in posting the credit as accounting for denials and short payments.
- Posting is done manually via data entry by clerical staff or through an uploaded posting file when electronic remittance information is available for automated posting. Posting files can be used to update the contract management system or the denial management system as well as the accounts receivable system.

Payment Services

- Bank lockbox services accelerate funds' availability by depositing checks into the clearing mechanism faster than providers can process such items internally. This is a mature service first developed in 1948. In recent years, banks have added the ability to image remittance data on high speed machines and present providers with the opportunity to post from images. More recently some banks have image or intelligent optical character recognition (IOCR) tools that turn EOB and check images into abbreviated 835 files (and may pull data from the provider's 837 to create HIPAA-compliant 835 files) for automated posting and population of denial management software with standardized adjustment reason codes mapped from proprietary adjustment reason codes on paper EOBs.
- Claim payments sent through the banking system allow the bank to pass 835 posting files to the provider, which the provider can post without human intervention because the bank ensures that the payment amount in the BPR segment of the 835 matches the payment received into the checking account. This eliminates the re-association task for the provider.
- Bank balance reporting information can be used to perform re-association services. In some cases, the bank will obtain ERA and warehouse 835s until the matching funds are received. In other cases the bank reports will be used by processors to provide re-association services.

10. Denial Management

Provider Process Steps

- Insurance payment denials can be interfaced to denial management systems or follow up can be generated off the standard code sets used on the 835. Combinations of the values in the code sets (group code, claim adjustment reason code and the remittance advice remark code) can be used to generate patient follow up. Institutions that can keep their denial rates at 3% or less are considered well run.

Payment Service

- Denial management systems require standardized adjustment reason codes. Banks providing the IOCR service can enable 100% utilization of denial management software by enabling 100% 835 formatted data for the provider.

11. Health Plan Follow up

Institution's Health Plan Processor Service

- Some payors send an unsolicited response (277) or a response (277) to a claim status inquiry (276). Typically, a comment is posted to the system recording the reason for it being paid, pending or denied.

Payment Service

- None

12. Secondary Billing

Many patients have secondary coverage. In these circumstances, the provider can submit a secondary claim for additional payment from payors. This can be done electronically in the 837 transaction, incorporating 835 information from a prior payment. This business process is often done on paper in part for lack of 835 information from all payors. The banking service that creates 835 data for all payors facilitates this ability to submit all secondary claims electronically, a HIPAA-mandated transaction called the coordination of benefits transaction or COB.

13. Patient and Guarantor Billing and Collections

Provider's Patient and Guarantor Process

- We are now at a point in the revenue cycle that if the provider has not been able to collect the deductible, coinsurance or co-payment or there are additional patient payment obligations due, the provider must send out a patient statement. There is a Patient Friendly Billing initiative by the Healthcare Financial Management Association (HFMA) to create a user friendly statement for the patient/guarantor. Failure to respond to an initial patient statement may result in the mailing of additional "third-party letters" to encourage payment.
- When the institution has contracted for patient payment lockbox services with their depository bank, a scan line is added to the coupon portion of the statement or the third-party letter. The bank's image technology can then use optical character recognition (OCR) to extract information from the scan line and the additional magnetic ink character recognition-encoded, or MICR-encoded, information from the patient's check (check number and amount) to send back on an electronic file to the provider for posting the accounts receivable. Image files of scanned items and checks are also available online or in a transmission as part of this patient payment lockbox service.
- Statement printing processors also offer the ability to put the statements online (not sent through the mail) so that a patient can go online, see his or her statement and make a payment through the ePayment service. The combination of these services allows the vendor of these services to send an electronic file to update the accounts receivable.

Payment Service

- A bank's patient lockbox service will create a payment file (Note: patient payments are not covered under HIPAA) with the payment information such as the payment amount, calculated prompt payment discount amounts (use the date on the scan line to determine if it has been paid in time), and identify payment types (credit card, debit card, etc.) for comment posting. Also, Web site information may be used to access the source document if the institution pays for the Web-based service that has the images of the check, coupon/stub and envelope with the post mark. The bank's Web service also can be used to send an image file to the processor for updating the patient's folder (see the statement filed and the payment made).

- Many banks offer an ePayment service that allows either the patient or an institution's representative to make a payment online. The ePayment service can send back a payment file that can be used to post the same transactions that are created from the patient lockbox service. The bank's Web service also can be used to send an image of the ePayment transaction to the processor for filing in the patient's folder. With more and more patients using online banking services, this mode of payment will become more and more popular.

14. Account Collections, Write-Offs

Provider Process Steps

- Before writing off an account to bad debt, institutions will give collection agencies an opportunity to work the accounts to see if they can collect the money from the patient.
- Processors can receive and post the bank lockbox bad debt payments to the bad debt accounts.

Payment Service

- The collection agency statement can have the scan line added so that the patient can send his or her statements to the bank lockbox for processing. An electronic file can be sent to the processor for updating the bad debt file.

Claim Processing Today

Claim Generation. In the first step of the patient/provider interaction, the patient's demographic, coverage and eligibility information is collected by the provider's registration system.

- 1) Insurance Information
- 2) Address
- 3) Physician's Name and location
- 4) Basic Data on Patient History and Experience

Upon discharge, a "claim" is created for the patient by the provider or a subcontractor. This claim is sent to either the patient or, more likely, to the patient's insurance provider (payor). It contains information specific to the patient encounter such as diagnostic (ICD9/ICD10) and procedure (CPT) codes. Additionally, the claim contains information that identifies the patient and the payor. This information is gathered and validated by a set of protocols and submitted to the insurance provider for billing and payment in settlement of the care given. The reimbursement process within the healthcare industry has evolved over many years and has achieved a high degree of national standardization in the form of commonly-used paper claim forms (CMS 1500s for professional claims and UB04s for institutional claims) and related electronic transaction standards. The healthcare industry was mandated to utilize ANSI ASC X12 837 transaction standards under HIPAA.

Claim submission is completed either on paper or electronically. If done electronically, the process is typically accomplished using the “837” claim transaction. The HIPAA-mandated transactions, with its numbered transaction sets (835, 837, etc.) are a subset of a much larger set of North American standards for electronic documents that includes many other transaction standards used in healthcare such as the purchase order (850) and invoice (810), used not only in healthcare but very widely in manufacturing and distribution industries.

CMS has been an early adopter of many of the X12 standards including adoption of the 835 standard for Medicare Part A claims payments in 1993, well before the HIPAA mandate. Providers wishing to continue with paper claims must solicit an annual exemption from their CMS payors.

See Tables A and B that describe the manual claims process and electronic process.

Claims Submission—Role of the Claims Clearinghouse

Since the 1980s, healthcare clearinghouses have been providing electronic data services to healthcare providers, health plans, pharmacies and other healthcare organizations. These electronic data services include moving financial, administrative and clinical data over to secure networks.

Virtually all healthcare constituents utilize a clearinghouse for these services. They have greatly simplified the complex process of handling electronic healthcare data. The clearinghouse provides a single point for an entity, such as a provider office, to send a file of transactions in whatever format their office system produces. The clearinghouse will, in turn, take the file, break it out by receiver (e.g. health plan, lab, etc.), apply any rules or edits required by the receiving end, translate the transactions into a HIPAA-compliant format, if required, and ultimately transmit the file to the receiving end in whatever format specified. Additionally, the clearinghouse will take any transaction acknowledgement reports generated from the receiving end indicating acceptance or rejection (with a reason) of the transactions, normalize them, and return them to the original sender.

Initially, EDI within the healthcare industry had been almost exclusively batch claims transactions. However, since the mid 1990s, the types of transactions have grown to include electronic remittance advice, eligibility, lab requests and results, e-prescribing and many others. This placed new demands on the clearinghouse infrastructure, leading it to evolve over time as a highly reliable and secure network supporting batch and real-time transmission modes, multiple transmission methods, and a high volume of all types of transactions.

One last point worth noting is that the clearinghouse world has an accrediting body called the Electronic Healthcare Network Accreditation Commission (EHNAC). This commission has developed extensive criteria from best practices that are used to assess an organization’s health and effectiveness. The criteria cover the following areas: customer

service, operational and marketing activities and HIPAA privacy and security. EHNAC accreditation assures customers they will receive a minimum standard of service and performance.

This evolution has created a firm foundation on which future healthcare initiatives such as HIEs or banking applications can be built.

Claim Payment Solutions. After the claim has been prepared by the provider, and processed by the clearinghouse, it is submitted to the payor. If all goes well, the payor accepts the claim and determines that the service is eligible for reimbursement. This reimbursement involves sending both information and money back to the provider. A claims payment requires both a remittance advice used by the provider to post the accounts receivable and a related funds transfer. Funds can be moved from bank account to bank account by using paper checks or various forms of electronic funds transfers; such transfers can be made by either Fed Wire or Automated Clearing House transactions. Only ACH transactions are suitable for electronic claim payments. The ACH system also plays a role when patients pay with credit/debit cards. While patient payments may originate in credit card or debit card networks, the financial settlement between the card processor and the (merchant) provider is always by an ACH credit.

Every bank in the United States connects to the ACH network, which is a closed, proprietary and completely secure network. Additionally, banks in the ACH network are governed by NACHA rules and other financial regulatory bodies. The Internet may be used to allow some payors to send 835s to their banks but such payment initiation is monitored with extraordinary precautions by banks at tremendous risk of fraud if security is not maintained. Secure FTP of 835 or NACHA files are a common methodology for initiating EDI payments.

Claim Remittance Solutions. Funding from a payor is accompanied by information that explains what is being reimbursed. In a paper world, there is no national standard for an explanation of benefits or remittance advice paper document. Naming conventions and the layout of information differ radically from payor to payor. Some payors developed proprietary electronic remittance information files in the 1980s but thanks to HIPAA, the vast majority of electronic remittance information is sent to providers in the ANSI X12 835 format. The HIPAA Implementation Guide to that transaction contains both required and optional data elements. Data elements must include patient account number, provider number, date(s) of service, the amount paid, amounts not paid and reasons for discounts or short payments.

In a paper-only system, a “check” with a printed statement explaining what claims are to be paid is generally referred to as an EOB or an EOP. The information is used to post accounts in the practice management or patient accounting system used by the provider—a very labor intensive process. The use of 835 electronic remittance advices (ERAs) eliminates most of the problems of non-standardized data elements. Because the use of the 835 is new to many payors, some issues of interpretation exist from payor to payor. Some payor ERAs may be considered faulty by providers and may require editing or

mapping. For providers receiving ERAs from multiple insurance plans, these unique mappings may become a difficult task. If each incremental payor agreement necessitates an additional data mapping exercise, this lack of standardization increases overhead expenses and the industry clearly needs to improve quality as measured by adherence to the 835 standard.

Integrating Banking Transactions

Financial institutions play a significant, but behind-the-scenes role in healthcare. All money must pass through a bank to complete a transaction. A few banks may act as claims clearinghouses, with far more acting as lenders and payment processors. They perform many IT functions that are beneficial to the provider. Below is a list of services provided today by financial institutions and used by healthcare enterprises:

- 1) Re-association
- 2) Lockbox services for retail (patient payments) and wholesale (health plan payments)
- 3) Online bill presentation and e-payment solutions
- 4) Consumer-driven health plans (health savings)

The Re-association Challenge

Feature Description. Re-association is the process by which providers deal with funds and data sent separately. The task of re-association does not exist in a world of paper checks and paper remittance advices. In a paper world, checks usually accompany remittance information and clerical staff can readily determine that the check amount matches the total amount paid referenced on the paper remittance advice. In a traditional lockbox environment, the bank deposits the check and often sends a photocopy of the check with the remittance information back to the provider; clerical staff then review documents in the traditional process, comparing the remittance advice total amount to the check copy total amount.

Doing business electronically may provide substantial benefits to a provider but may add complexity when payors separate data and dollars. When a payor sends ERAs or electronic funds transfers, there are far more options than the postal service. Each has its own set of costs and benefits for payor and provider.

When a payor opts to send ERA data, that remittance information is no longer available on paper for the posting staff to read and compare to the paper check. In fact, as an X12 835 EDI file, it is a string of data and delimiters that makes reading by non IT staff difficult even if printed. Some providers use a small program that turns the 835 into a human readable file and manually enter the data into the system rather than using an automated posting routine.

The problem of re-association is compounded by the fact that payors may have production schedules where the check or EFT may arrive days later or earlier than the 835. Providers receiving ERAs without an automated re-association service involving

their banks perform extensive searches using spreadsheet reconciliation logs to ensure that all payments received are accounted for.

Re-association between payment and ERA can be substantially automated by various bank services but it requires knowledge of how information is captured in the banking system and reported by banks to their customers. How should providers “look for” the relatively few check payments that relate to ERA among all the other checks? The answer is to utilize bank data capture and reporting tools so that bank reports can be reviewed to match ERA and check payments. This can be done manually or in an automated fashion with banking services, developed for this need over the last 20 years and fully supported by the ANSI ASC X12 835 standard.

The key to re-association is matching data that accompanies payment with data that accompanies remittance information. The 835 contains a trace segment, a field of information expressly designed to support re-association. The trace segment contains a unique number that is within the remittance advice and is identical to information that accompanies payment. In the case of a check, it may be a check number. In the case of an EFT, it will be an EFT identification number plus other information, dependent on how much additional information the payor sends the provider through the banking system.

Providers performing manual deposits to a bank account that lump multiple checks into a single deposit must manually review bank images to find the check in question. The challenge facing the provider is how to work with his or her bank to capture and report data on a check or in an EFT as well as facilitate reporting and re-association tasks. Providers whose banks capture check number, date and dollar information for reporting can obtain more granular data for re-association in an automated report from their bank. That same reporting functionality can pass information sent with EFT so all payment transactions are reported in one place for re-association with ERA sent separately.

Further explanation of how data moves with EFT may be helpful here. There are two ACH formats authorized for use in the HIPAA guideline for the 835 transaction: CTX and CCD Plus (CCD+). The CTX format is supported widely in the banking industry for business-to-business (“B2B”) payments. It allows for funds transfer and inclusion of remittance data in the same file. The CCD+ enhances the CTX with an “addenda record” for transmission of limited X12 information. This addendum facilitates re-association. Both these transactions are used for the two X12 payment standards, the 820 and 835. They provide the overwhelming majority of B2B EDI payments in the United States.

When payors use these two authorized ACH formats specified in HIPAA, banks can assist in automating the provider’s re-association challenge. If the banking system is used to deliver ERA data via the CTX format, the bank service includes the step of reconciling the dollar amount deposited in the funds transfer with the information provided in the 835 transaction. When the banking system is used in this fashion, there is no re-association challenge for the provider.

When funds are sent separately, re-association is accomplished through what is called the trace (“TRN”) segment in the 835 transaction file described earlier. The NACHA CCD+

format contains the trace segment that is identical to the TRN segment sent in the 835, delivered either directly to the provider or through a clearinghouse. Banks may receive an ERA on behalf of the provider and “warehouse” and wait until a matching EFT arrives. Once both information and money are in hand, the bank then delivers the 835 transaction file to the provider for posting. Some payors may send the header information of the 835 in the CTX format. While this still requires “re-association,” the additional information in the header area of the 835 identifies the payor more completely and may provide the contact name and phone number should something go wrong with the transaction.

In some rare cases where the monetary amount is different from the ERA total, the bank can adjust the paid amount total in the 835 file to accurately reflect the funds transfer. In all cases, the provider is passed a file that can be posted with no manual re-association tasks, fulfilling EDI’s goal of moving data between payor and provider without human intervention.

Banks may offer Web-based viewing to see the status of the 835 files being held. This allows providers to check on pending claim settlements that have not been funded.

Benefits to the Provider

- Bank reporting supports manual re-association of check and EFT to ERA for providers with limited ERA transaction volume.
- Higher value added re-association services eliminate the labor-intensive re-association service it is outsourced to the bank.
- The accounts receivable is not updated until the money is deposited in the bank.
- Provider has a Web-based view of their held and released activity.
 - 835s received without payment
 - Payments received without 835s
 - Payments released for processing (by match or default)
 - History report
- Provider will have faster notification of denials, enabling the provider to begin an appeal sooner, thus reducing A/R aging.

Patient/Retail Lockbox

Feature Description. A good percentage of all patient payments today are still paid by the patient using a document sent in the mail by the institutional/physician provider. The document sent by the provider could be a statement or third-party letter. Each document has a perforated stub, also known as a coupon, on its lower section. The documents contain information integrating the payment into the accounts receivable file. Information such as the patient number, payment amount and statement date, whether service was inpatient or outpatient, etc., are on the payment stub. Often, this data is incorporated in a row of numbers and letters known as the OCR scan line if needed by the provider’s posting process. The patient mails the coupon along with the payment (check or credit card information) in a return envelope to a post office box rented by the bank.

The bank periodically collects the envelopes from the post office and scans each document. In high volume situations, extremely automated high speed equipment is used. Checks are endorsed and deposited. Images of the checks and statements are created. An electronic file is produced, conveying information that matches the amount of the deposit with the data on the payment coupon. This file is sent electronically to the provider, whose accounts receivable are updated. At day end, the money is available to the provider, and the account receivable balances are reduced.

One benefit of this scanning effort is that the lockbox documents are available on a Web site for the provider's viewing and downloading; image files are supplied through the bank's Web site. Alternatively, it will send documents to the provider, who will place them in his or her imaging system. The document sent electronically by the bank is an 8 ½ x 11-inch document containing the envelope, check and stub/coupon. This can then be used by the provider to automatically file a copy in the patient's folder and a generic pay date folder.

Benefits to the Provider

- The accounts receivable ledger can be updated at the same time the money is deposited and available in the bank.
- The manually intensive process of opening envelopes, creating a deposit slip and updating the receivable is outsourced to the bank.
- Outsourcing the processing to the bank saves one or more days for depositing the money and updating the accounts receivable.
- Experience demonstrates a 99% accuracy rate with the bank's lockbox process.
- Lockbox services offered by the bank can perform the following functions:
 - Create the patient payment from the check so it can be posted by the provider
 - Post a comment containing the patient's check number (from the MICR encoded line on the patient's check) or the patient's credit card information.
 - Create the credit card deposit and give the credit card information on the electronic file so that it can be posted at the credit type level (American Express, Visa, MasterCard, etc.)
 - Create the prompt payment discount from the date on the scan line
 - Eliminate any manual intervention except to deal with the exceptions (patient does not return the coupon)
 - Send an electronic image along with the payment file to update the document imaging system.
 - Use the bank's image platform to view all source documents used to create the electronic file and research any errors. The Web site has a separate section for correspondence scanned as well.
 - One lockbox can be used for multiple providers. The bank can create separate deposits from an identifier on the document's scan line. This saves monthly recurring costs for the provider.

Insurance/Wholesale Lockbox Using Intelligent Optical Character Recognition (IOCR)

Feature Description. Most of the major non commercial insurance companies can produce 835 transaction files electronically. Examples are Medicare, Medicaid, Blue Cross/Blue Shield plans and the major commercial insurance companies such as Aetna, Cigna and United Healthcare. All health plans are mandated to do so under HIPAA.

In reality, a significant number of payors still do not send electronic 835 files. Many have legacy systems that cannot produce the information to make the files HIPAA compliant. Some workers' compensation and property and casualty companies were exempted from HIPAA and remain paper-based. Some payors also provide more information on the paper EOBs than on the 835.

Banks have created a solution for managing the paper EOB from payors by using sophisticated scanners that can take the paper EOB and create an 835 data file from the EOB scanned image. This service may utilize the provider's claims files, which are obtained from the bank to supplement the data in EOBs that lack service codes from the original claim. Additional value-added functionality stems from the bank's support of the ANSI X12 codes used to explain why a claim is denied or not paid in full. Under HIPAA, the 835 file must provide two codes, the Claim Adjustment Reason Code ("CARC") and Remittance Advice Remark Code. However, some of the smaller payors, with legacy systems, do not provide this information in a HIPAA-compliant format. These scanning solutions will take a paper EOB, recognize the payor's old proprietary adjustment reason codes and translate them into data that conforms to HIPAA standards.

From these files and the paper EOB, banks can create a HIPAA-compliant 835 file (with line item detail) and send it to the provider for processing—just as if it were created and sent by the payor.

Benefits to the Provider

- Automates the manual posting of EOBs, saving time and labor costs.
- Allows the bank to create an 835 with payments and denials to support a standard integration to accounts receivable as well as capture denials in a standard way for all payors.
- Updating accounts receivables and depositing payors' checks can be synchronized to simplify the bank statement reconciliation.
- Outsourcing the processing to the bank saves one or more days for depositing payor's checks and updating accounts receivables.
- Experience demonstrates a 95% accuracy rate with the bank's lockbox process.
- Lockbox services offered by the bank can perform the following provider integration functions:
 - Create a new template when a payor sends a new EOB form.
 - Provide an automated interface to the provider's denial management system.
 - Eliminate any manual intervention except to deal with the exceptions.

- Send an electronic image along with the payment file to update the document imaging system.
- Use the bank's image platform to view all source documents used to create the electronic file and research errors. The Web site also has a separate section for correspondence scanned.

Online Bill Presentation and ePayment Systems

Feature Description. Today, banks (allied with vendors) offer a solution for putting the provider's statements online for viewing and allowing patients to make payment through the Web site. The bank offers a Web site with the same color scheme and logos as the provider's Web site and the payment terms available to the patient. The patient logs on to the provider's Web site, can review a statement, and with a click, will be taken to a secure Web site to make a payment.

Payments are typically made by debit or credit card. At day's end, the bank sends an electronic file to the provider for integrating the payment and payment terms.

Banks will also make available an image of the financial terms from the Web site for filing in the provider's imaging system.

Benefits to the Provider

- Solution to capture payments. Many patients prefer paying through their own Web site or at a provider's onsite kiosk, rather than sending a check to the provider's lockbox. At some point in the future, more patient payments will be made than through today's lockbox. Hospitals define payment terms and methods on their Web sites.

Consumer Driven Health Plans

Feature Description. Consumer-driven health plans (CDHPs) are high deductible health plans that combine the availability of tax sheltered funds called health savings accounts. Banks play a major role in CDHPs by maintaining the bank accounts for the individual subscriber, which are usually tapped through the use of debit cards. From the bank's standpoint, these accounts are checking accounts with debit card access. The normal way of depositing money into the account is through a payroll deduction.

The patient subscribes through a payor to a plan that authorizes providers to either view the account for available funds or extract funds from the HSA to pay the patient obligation.

Provider Benefit

- Monies are available to pay the patient obligation by the subscriber. The subscriber uses his or her card to pay the provider.

- When the final bill is produced, payors will adjudicate the claim. They will take the funds from the HSA account if authorized by the subscriber. This is known as integrated financial settlement. Some payors will combine it with the payor's contribution to the total reimbursement payment. A CARC should be used to identify the patient payment amount of the CDHP payment. The provider must take the amount of the CARC out of the total payment and post the insurance payment to the insurance plan and the patient payment to the patient obligation.

Future Predictions

In response to the rising cost of healthcare and the added emphasis on quality of care, healthcare providers are integrating Web-enabled/electronic solutions into their administrative, diagnostic assessment and care plan protocols. These new developments necessitate a fresh look at existing solutions and understanding the current gaps with security and privacy. HIPAA took a necessary first step toward a set of standards for protecting patient records. This has fostered a level of collaboration and cooperation between the public and private sectors, and between healthcare providers and the technology/service vendors.

Financial institutions provide services for payment clearing and settlement to the healthcare industry. Responsibility comes with these services being a "trusted party." Such a role requires compliance with regulations designed to protect clients' records and the added interest of giving the assurance of payments. The nature of Web-enabled electronic transactions and the use of the internet Infrastructure are new. These new conduits require a higher level of security management to not only protect payment transactions, but also the data associated with the transaction. This is commonly referred to as remittance information, the paid claims data that describes financial transactions.

Future Considerations as Financial Institutions Conduct Web-enabled Payments

The core business service financial institutions provide to its customers is the assurance of payments. Payments are delivered and processed over multiple payment networks, utilizing diverse solutions such as the "paper" check, "e-checks", debit and credit cards and the "Federal Wire" systems. Clearing and settlement of these payments is achieved through the existing ACH System. Under the purview of the Federal Reserve System, which was created in 1913, the ACH system facilitates movement of funds in a concise, predictable and efficient manner. Financial institutions and the Federal Reserve are aware that on the horizon, the use of alternate electronic means of facilitating payments offers challenges the entire industry must meet in order to perform the vital function of reliability of payments. If this payment system is challenged in any way, trust in the system will be lost by the general public. Today, trust, a significant concern, can be threatened through any number of issues including security, privacy and corruption. Any break in this trust and confidence in our nationwide economic system will significantly impact this system and threaten collapse. The increase in the number of Web-enabled or "Internet" payment solutions processed by financial institutions has already changed the infrastructures of these payment networks. These networks had to shift in order to accommodate interoperability and integration of Web-enabled transactions to provide

services which facilitate straight-through-processing (STP). As industry after industry took action to improve their efficiencies and cost reductions, demands were placed on banking services to process multiple payment solutions and to provide additional services to further automate the clearing and settlement of payment processing.

The current EDI solutions were really designed and utilized in a portal/proprietary environment. These Web-enabled solutions are now being used over the Internet, which was designed to easily and cheaply share data between business partners both known and unknown. The Internet was not originally constructed with functions supporting security and privacy of data sharing; financial institutions are legally mandated to provide such criteria. The problem of transaction corruption does not typically occur in sharing data between partners in a network bound by either contract or negotiated agreements. It most likely occurs when the data is shared between networks or communities of “trust” without some neutral party providing for risk mitigation as related to the assurance of payments. Since financial institutions now have the responsibility of providing for this payment assurance over a multitude of emerging payment solutions, an increasing body of study and evidence is emerging that attempts to provide a framework for policy, rules and enforcement to provide more secure Web-enabled payment solutions. The following section outlines some of the issues and challenges in this area to encourage future collaborative discussions between public and private sector participants on healthcare-related transactions.

Payment Challenges for Financial Institutions

Financial institutions share with healthcare providers the role of “trusted party” and legal and regulatory requirements to provide for client security and privacy. In a number of standards organizational bodies (ANSI X9/OMG) and “proof of concept” consortia (Financial Services Technology Consortium/FSTC) in various projects, it has been noted that the role of financial institutions is to:

- Provide for the risk of identity management.
- Provide for mitigation of risk in Web-enabled transactions.
- Provide for the assurance of payments.

Identity Management and the Use of “Credentials”

Financial institutions have a 300-year-old history of being able to identify their clients through various means. Today, a “credential” refers to an electronic method linked to a set of protocols supporting the exchange of documents and other information. This credential is verified to be accurate and recognized when coordinated with a set of agreed upon policies to form a “trust framework.” Consortia such as the Liberty Alliance have developed a “trusted framework of assured identity” that financial institutions and standards development bodies such as the American National Standards Institute (ANSI) have agreed to use when developing governance of Web-enabled transactions.

The important part of the presentation and acceptance of this “credential” within the beginning of the transaction establishes a mutual authentication between the two parties and mitigates the risk of fraud. Generally, the strength level of the credential should be

directly related to the value or risk of the transaction. The use of “user identification” and “password” function well in a closed network and perhaps in a set of low value Web-enabled transactions. Higher value transactions in financial institutions work in multiple venues and must be mapped to the risk level. To understand the concept of mapping the level of risk to the strength level of the credential, the National Institution of Standards and Technology (NIST) has published “NIST 800-63” as a standard for running four levels of defined risk:

Level 1: Low value and perhaps “user ID and password” would suffice.

Level 2: Low value and determined in value to require PIN/password.

Level 3: High value and “business risk” mappings to determine for the enterprise, perhaps a set of multiple digital solutions.

Level 4: High value and mapped to require “strong” credential solutions.

Additional types of credentials being considered by financial institutions to provide the appropriate strength level are:

- Biometrics
- WS Federation
- Liberty Alliance, SAML 2.0
- PKI Certificates
- Shibboleth

In order to facilitate the use of an application as related to a payment solution of a group of rich and diverse payment networks, the appropriate strength level of the credential must first be presented and accepted. This must be accomplished based upon a trust framework to provide assurance of identity and a set of agreed upon policies and rules which are articulated, understood and enforced. The use of standards to support interoperability and integration is required for financial institutions to provide the appropriate level of service, privacy and security as well as process multiple web enabled solutions over multiple networks and multiple applications. Financial Institutions recognized that a more public/private collaborative environment is necessary to provide for the testing of high volume payment transactions for the development of benchmarks, methods and standards. These are necessary to provide the assurance of actually providing the level of service appropriate to multiple industries. Healthcare as an industry provides such an environment but there must be a more “cross-industry” set of activities, which might involve multiple venues as the transaction chains or points of healthcare involve multiple industries. Payment is one part of that transaction chain and facilitates multiple industries as financial institutions provide payment services to many components of our economy.

Key Areas with Anticipated Change and Advancement in the Future

Technology Advances

- Technology is anticipated to grow tenfold in the next 20 years.

Payor/Provider Systems

- Payors/providers will no longer be able to say “I have a Legacy System” and not be able to support the HIPAA transactions in 2012. Cost is a major issue surrounding the implementation of the X12 transactions under HIPAA.
- Real Time Adjudication (RTA) of 837 claims is used in the payment of pharmacy claims today. It is anticipated that many payors will allow a physician’s RTA when he or she enters the claims online.
- Growth in the functions of these systems is anticipated in the future.

Payors

- Move from legacy systems by 2014.
- Growth of personal health records transported from payor to payor in 2009 (X12).

Regulatory Compliance

- HIPAA2 and implementation: The timeframe for rolling out a new version of HIPAA is very extensive. It takes getting the 835 standard (all HIPAA transactions at the same level) approved by X12, reviewed and approved by the healthcare industry in order to set implementation dates. Today, organizations like WEDI and NCHICA are trying to reduce the steps to roll out the next cycle.
- Implementation of the International Classification of Diseases Version 10 (ICD-10) is estimated to follow the implementation of HIPAA2 by two years.

Networks

- Traditional methods of connectivity through FTP and VANs will be replaced by the Internet.
- Banks are investigating the use of ATMs for moving the health record.

Terminals/Products

- Kiosks are being introduced to streamline patient registration processes. Kiosks are used to collect money at various registration areas.
- Scanning devices for credit cards and debit cards to allow the capture, deposit, processing and integration of patient payments.

Consumers

- Some insurance companies allow their members to have access to their health records online. When a member changes insurance plans, the X12 standard transaction allows insurance companies to exchange information electronically.
- Electronic health records have been endorsed by the federal government to reduce the administrative costs of healthcare.

Frequently Asked Questions

Question: As a provider, if I want to take advantage of the services described in this document, what do I need to consider?

Answer: To outsource the services to the bank and the vendor, you need to know their costs versus the savings and additional automation features provided by the service.

Return on investment items are:

- Cost for the FTEs performing the function
- Speed to manually process versus automation
- If imaging is involved, the cost of manually imaging versus automatic filing
- In the case of lockbox and ePayments, the timing of the deposits

Question: As a provider, if my bank does not offer these services, can I get them from another bank?

Answer: At the option of the institution's management, they may contract with a separate bank for just that service. The relationship with the bank normally is the determining factor.

Question: Do all banks offer the services described in this document?

Answer: If a bank has committed to understanding and providing services to healthcare institutions, they may provide all or part of the services described. More and more banks realize the need to support their healthcare customers with services like the ones described. Many smaller hospitals will utilize the lockbox services of a bank rather than develop mail and check handling and EOB imaging and conversion to 835s themselves.

Question: Do banks have healthcare representatives?

Answer: The larger banks have healthcare divisions with treasury management representatives that support the services described.

Question: As a provider, will my bank work with my hospital information system (HIS) to implement the services?

Answer: Different vendors have different integration solutions. You will need to contact your HIS vendor to see if they can receive a file from the bank and create the integration transactions that you require (i.e. post payments, prompt payment discounts, payment type, etc.).

Table A: Revenue Cycle Diagram for an Institutional Provider



Table B: HIPAA Standard Transaction and Code Sets

Providers	Transaction Standards	Payors	Employers
Eligibility	<p>270 Eligibility Inquiry →</p> <p>271 Eligibility Response ←</p>	Enrollment	<p>834 Enrollment ←</p> <p>820 Premium Payment ←</p>
Referrals Authorization	<p>278 Referrals/Authorizations ↔</p>	Referrals Authorization	
Claim Submission	<p>837 Claim →</p>	Claim Acceptance	
Claim Status Inquiry	<p>276 Claim Status Inquiry →</p> <p>277 Claim Status Response ↔</p>	Claim Status Response	
Accounts Receivable	<p>835 Claim Payment ←</p>	ERA/EFT	

Glossary of Terms

Term / Acronym	Description
835	This is the ANSI ASC X12 transaction set code number for the transaction set called the “Claim Payment/Remittance Advice. The 835 can be used to initiate a payment or send a remittance advice or both, together or separately.
837	This is the ANSI ASC X12 transaction set code number for a national standard used as a standard format for electronic claims. Providers use the 837 file to submit billing and encounter information to payors. They send it either directly or via intermediary claims clearinghouses. Payors use the 837 to transmit claims to each other.
ASC X9	Accredited Standards Committee X9 (ASC X9) has the mission to develop, establish, maintain and promote standards for the financial services industry in order to facilitate delivery of financial services and products.
Bank / Financial Institution	Used interchangeably.
Denial Management	Denial management is a process for providers dealing with remittance transactions that indicate a claims denial or underpayment. There can be denial management software tools to automate the denial management process for tracking and monitoring denials. The X12 835 code sets for claims adjustments are used by payors to describe to the provider the reason for denial in an 835 Electronic Remittance Advice.
Document Imaging	Process where paper documents (claim forms, checks) are scanned and stored electronically.
EDI Capable	Banks who have Electronic Data Interchange solutions.
Electric Funds Transfer	Electronic Funds Transfer can be made in two ways. The first, FedWire, is a real time transfer of funds from the Fed Account of one bank to the Fed Account of another. ACH or automated clearing house transactions are more similar to checks in their cost and timing. They are “next day” items and can be used to send both electronic funds and remittance and trace number information in X12 standards between payors and receivers.

Explanation of Benefits (EOB)	Explanation of payor's claim adjudication that is sent to the patient. This term is often used by providers in the remittance information sent via paper claims payment.
Electronic/Online Bill Presentment Payment (EBPP)	Web access to statements for viewing and making payment.
Electronic Remittance Advice (ERA)	Electronic Remittance Advice is an electronic file that is sent from the health plan payor to the provider that can be used to post and close accounts receivable. The X12 standard for electronic remittance information is the 835 standard.
ePayments	Payments made by the patient or authorized hospital staff using the provider's Web site.
Financial Services Technology Consortium (FSTC)	FSTC members, including financial institutions, other industry groups and vendors collaborated in non-competitive research and development of inter-bank technical projects.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, among other things, required the Department of Health and Human Services to promulgate healthcare transaction standards for the automation of the claims process.
HIPAA Transactions	Electronic standard transactions that were approved for use under the HIPAA legislation. They support the steps in the revenue cycle and automate the workflow. HIPAA transactions apply to insurance payment transactions only. Financial institutions use both the 835 and other X12 and industry standards to facilitate funds transfers and bank reporting.
HRA	Health Reimbursement Account
HSA	Health Savings Account
ICR/IOCR	Intelligent Character Recognition/Intelligent Optical Character Recognition. Used to create templates to read the data off the paper EOB. It is used to convert a paper submission into a HIPAA compliant 835 electronic file.

Image Vendor	Vendors who provide the IOCR technology
Insurance/Wholesale Lockbox Service	A bank lockbox that receives explanation of benefits (EOB) and checks from the insurance company to cover their portion of the patient's claim. It receives paper documents and uses IOCR/ICR image technology to create the 835 electronic file.
MSA	Medical Savings Account
Object Management Group (OMG)	OMG is an international open membership, not for profit computer industry consortium. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.
Optical Character Recognition (OCR)	Used to read the scan line on patient statements & MICR line on the patient's check
Payor Template	Created by the IOCR image vendor to retrieve information from the paper EOB to create the 835. The bank account number or payor logo on the payor's check is used to retrieve the payor template.
Patient Friendly Billing	HFMA Initiative to make the statements sent to the patient easy to understand. It provides guidelines used by forms vendors when creating a patient statement.
RA	Paper Remittance Advice, a common term used by the healthcare community, typically refers to a paper document containing the results of the adjudication/payment process sent from the payor to the provider. This term occasionally is also used for the electronic remittance.
Re-association	The process to match the Check/EFT Number and Dollar Amount on the 835 to the related financial transaction.
Revenue Cycle	Time from scheduling a patient visit (or emergency) through treatment, billing, collection of payment, and account closure or account write-off.
The Liberty Alliance Project (LAP)	The Liberty Alliance Project is a consortium of commercial and non-commercial organizations working to support the development, deployment and evolution of an open, interoperable standard for federated identity

management.

X12

The ANSI (American National Standards Institute) Accredited Standards Committee (ASC) X12 was chartered in 1979 to promulgate national standards for corporate document exchange needed to conduct Electronic Data Interchange. There are hundreds of X12 standard electronic document formats called transaction sets. These include transactions used by financial institutions, providers and payors, some of which are mandated by HIPAA.



Credits

Members of the HIMSS 2007 – 2008 Financial Systems Financial Banking and Healthcare Task Force, who spearheaded the development of this white paper, include:

<p><u>Douglas Beaupit</u> Software Product Analyst Siemens Health Solutions Email: douglas.beaupit@siemens.com</p>	<p><u>Matthew Guldin</u> Industry Analyst Frost & Sullivan Email: matthew.guldin@frost.com</p>
<p><u>Patricia Hewitt</u> Product Manager Siemens Health Solutions Email: patricia.hewitt@siemens.com</p>	<p><u>James Moynihan</u> Senior Vice President U.S. Bank Email: james.moynihan@usbank.com</p>
<p><u>Ted Perkins</u> Consultant Children's & Women's Physicians of Westchester Email: ted@tedperkins.com</p>	<p><u>Michael Talley</u> Systems Analyst University Bank Email: mtalley@university-bank.com</p>
<p><u>Samir Vyas (Chair)</u> Director - Business Development Reporting House Email: sam.vyas@reportinghouse.com</p>	<p><u>Pam Matthews, CPHIMS, FHIMSS</u> Senior Director, Healthcare Information Systems HIMSS – Staff Support pmatthews@himss.org</p>
<p><u>Holly Gaebel</u> Coordinator, Healthcare Information Systems HIMSS – Staff Support hgaebel@himss.org</p>	

The inclusion of an organization name, product or service in this publication should not be construed as a HIMSS endorsement of such organization, product or service, nor is the failure to include an organization name, product or service to be construed as disapproval. The views expressed in this white paper are those of the authors and do not necessarily reflect the views of HIMSS.