Networks for Health Information 3

Information technology can be used to automate many administrative processes in the health care system, including transactions between those who provide health care services and those who pay for them. The general term *electronic commerce* is used in the chapter to describe the automation of business transactions and the direct computer-to-computer exchange of information, business documents, and money.

This chapter examines electronic communications between providers and payers (including interactions with electronic medical claims companies, value-added networks, clearinghouses, and others that facilitate this communication). It also discusses electronic commerce between health care providers and medical/ surgical manufacturers and distributors, as well as between pharmacies and both pharmaceutical distributors and claims payers. The role of communication networks in facilitating the exchange of health information among health care providers, payers, and others on a community-wide or regional basis is examined. Figure 3-1 illustrates some of the directions in which information needs to be exchanged, or transactions need to be effected, among the various components of the health care delivery system.

Electronic communications can free administrative information from paper, allow it to be processed automatically (without human intervention), and permit it to be readily reused for a number of related purposes. In many cases, it appears that electronic commerce can provide some cost savings to health care system participants and to the system as a whole. Realizing those savings requires investment in equipment and training, as well as industrywide agreement on and compliance with standards for the format and content of messages. The chapter reviews some of the research on costs and cost-effectiveness of various uses of elec-

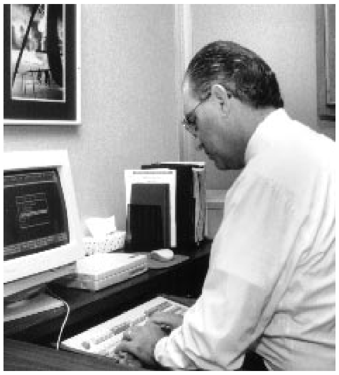
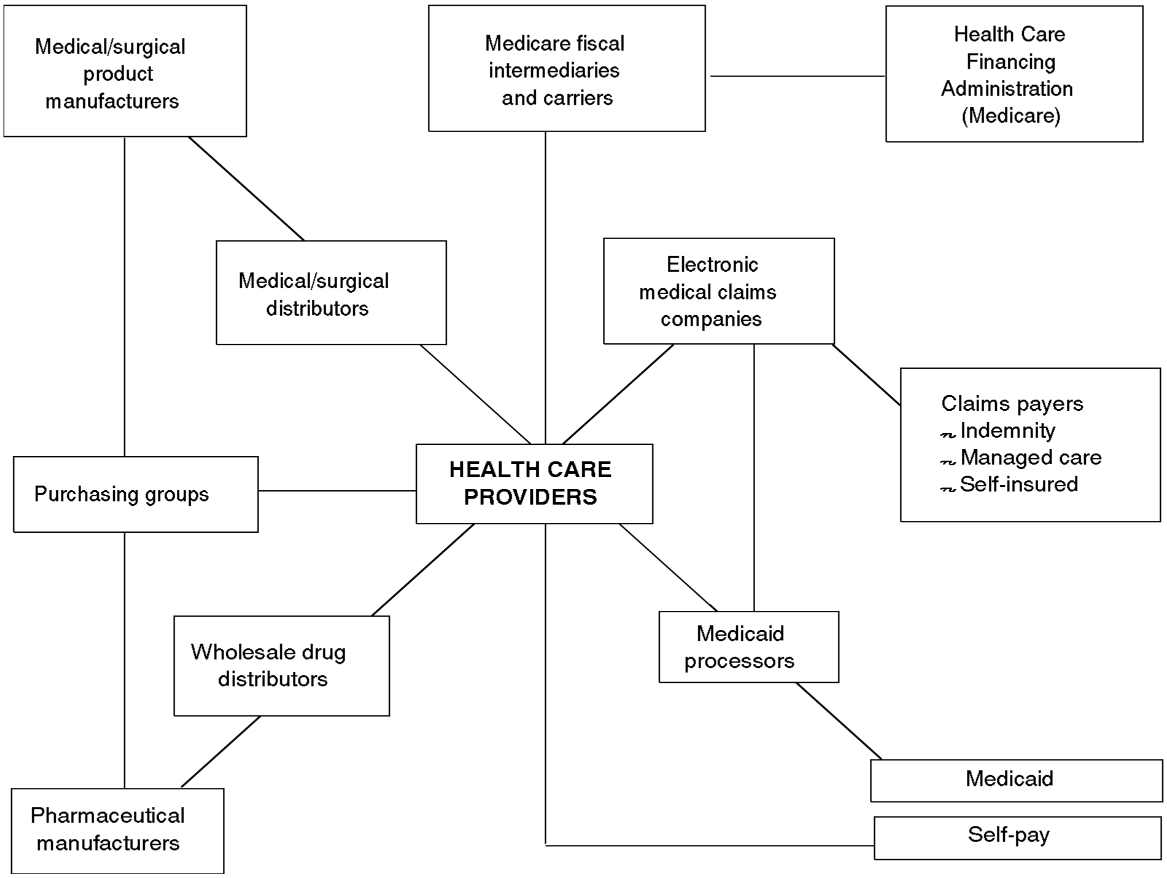


FIGURE 3-1: Health Care Industry Trading Relationships


Medical/surgical product manufacturers
Medicare fiscal intermediaries and carriers
Health Care Financing Administration (Medicare)
Medical/surgical distributors
Electronic medical claims companies
Claims payers
Indemnity
Managed care
Self-insured
Purchasing groups
HEALTH CARE PROVIDERS
Wholesale drug distributors
Medicaid processors
Medicaid
Self-pay
Pharmaceutical manufacturers

SOURCE: J. Moynihan and K. Norman, "Health Care EDI: An Overview," *EDI Forum*, vol. 6, No. 2, 1991, p. 11.

tronic commerce and regional networks in health care. In addition, it outlines some of the overarching issues that affect the adoption of the technology by participants—industry fragmentation, the slow development of standards, the fragmented regulatory and policy environment, as well as concerns about privacy, confidentiality, and security of health information in a networked environment.

ADMINISTRATIVE SIMPLIFICATION

Administrative simplification has come to mean streamlining and standardizing the transactions between health care providers and payers to reduce costs. The administrative costs of providing health care have been estimated at between $108 billion and $135.1 billion per year in 1991,[1] or between 12 and 15 percent of the health care bill. Es-

[1] Lewin-VHI, "Reducing Administrative Costs in a Pluralistic Delivery System Through Automation," prepared by A. Dobson and M. Bergheiser for the Healthcare Financial Management Association, Apr. 30, 1993.

timates of annual savings that could be realized through increased use of information technology to streamline administrative functions have ranged from $5 billion to $36 billion,[2] or enough to reduce administrative costs between 0.5 and 3.6 percent.

Administrative simplification generally means not only standardizing forms, procedures, and information requirements, but also moving to electronic technologies from paper-based transactions and recordkeeping. This chapter will review some of the technological, legal, and economic issues involved in administrative simplification. It also discusses more generally the concept of "electronic commerce," the exchange of business information and money through computer networks, and specific tools for electronic commerce such as electronic data interchange (EDI). (See boxes 3-1 and 3-2.)

In the traditional "fee-for-service" health care delivery system, the health care provider performs services for the patient and then submits a bill to the patient. If the patient is insured, either the provider or the patient will submit a claim to the payer (insurer) to reimburse the patient or to pay the provider directly on the patient's behalf. The information exchanged between care providers and payers (insurers) can be very complex. The information that a payer requires a health care provider to furnish in order to get a claim paid depends not only on the payer's policies, but on the laws of the states in which the payer, provider, and patient are located. In addition, because many patients are covered by more than one insurance plan, there may be secondary or tertiary payers involved in paying a single bill. From the provider's point of view, getting that bill paid may be quite burdensome. The various payers may not only require different information, in different forms, but may also require the provider to furnish information about the other payers in order to coordinate benefits for the patient.

Several studies of health care administrative costs have suggested that the large number of different payer institutions (over 6,000) and the variety of formats in which they request claim information are factors in making the cost of health care administration much higher for the United States than for other industrialized countries.[3] A government-mandated change to a single-payer system might reduce these costs, but such an action appears unlikely. Administrative simplification, through the introduction of electronic transactions and through standardization of transactions and processes, may offer a way to achieve more modest savings.

Many managed care companies now perform the functions of both payer and provider. However, this does not necessarily reduce the number of transactions or ensure that administrative simplification will be achieved simply by enrolling most of the population in health maintenance organizations (HMOs) or other managed care systems.[4] While some interorganizational transactions are eliminated, they are often replaced by analogous exchanges of information within the managed care company. In addition, managed care organizations are "information hungry" and are creating new management information exchanges between their "provider" and "payer" components.

In some HMOs, where patients are served only by providers employed by the HMO and where all financial risks (the insurance functions) are assumed by the HMO itself, there is usually little need to submit claims to payers, except for occasional referrals to outside specialists. However, managed care is coming to have forms. Managed

[2] Project HOPE Center for Health Affairs, Bethesda, MD, "Estimating the Cost-Effectiveness of Selected Information Technology Applications," unpublished contractor report prepared for the Office of Technology Assessment, U.S. Congress, Washington, DC, March 1995.

[3] U.S. Congress, Office of Technology Assessment, *International Comparisons of Administrative Costs in Health Care,* OTA-BP-H-135 (Washington, DC: U.S. Government Printing Office, spring 1994).

[4] For more description of managed care, see box 1.1.

BOX 3-1: EDI and Electronic Commerce

Electronic Data Interchange (EDI) is defined as the application-to-application interchange of business data between organizations using a standard data format.[1] A computer *application* is a software system that performs work. Information is routed through telecommunications networks, received by an organization's EDI system, and processed by its computer applications—all without human intervention. Redundant data entry is thus eliminated, which increases the accuracy of information and reduces administrative costs.

Organizations doing business with one another are called *trading partners*. Companies have used EDI to reduce the costs of exchanging and processing documents for more than 25 years. In the last several years, however, companies and consultants have placed EDI into a larger context called *electronic commerce*.

Electronic commerce is a management concept in which all information flows between and within organizations through networked computer systems. Work can be done in ways that differ from a paper-based system. In electronic commerce, for instance, a process made up of discrete tasks may be performed as a series of parallel tasks. Only one person can work on a paper document at a time. When the information contained on that document is freed from the constraints of paper and ink and is available in electronic form, several people can access, use, and transform the information at the same time.

EDI is not a concept like electronic commerce; it is a technology consisting of rules and standards programmed into computers. One could say that EDI is to electronic commerce as statistical process control is to total quality management; that is, EDI is one of the tools required to put the management concept of electronic commerce into action.[2]

Standardization is the key to EDI. Computers cannot process the information that moves between organizations electronically unless it is encoded in a manner that the computers at both organizations can recognize. In other words, both computers must be able to *speak the same language*. In linguistic terms, they must follow standard usage. EDI provides a set of rules, grammar, and syntax that forms the basis of standard usage in the electronic exchange of business data. EDI is both the means and the language that computers use to "talk business."[3]

SOURCE: C. Canright, "Electronic Commerce and Networking in Health Care," unpublished contractor report prepared for the Office of Technology Assessment, U.S. Congress, Washington, DC, Jan. 31, 1995.

[1] C. Canright, "The Problem of Data Mapping," *EDI Executive*, vol. 4, No. 6, June 1989, p. 1.

[2] G. Gerson, Sr., "Interview with Captain Bruce Bennett, USN, Executive Agent for Electronic Commerce, United States Department of Defense," *EDI Forum*, vol. 6, No. 3, 1993, p. 42.

[3] R. W. Notto, "EDI Standards: A Historical Perspective*," EDI Forum*, vol. 1, No. 1, 1988, p. 120**.**

care organizations can have a variety of relationships with providers (e.g., they may be employees, or they may accept patients under exclusive or nonexclusive contracts). They may also have a variety of relations with payers, assuming some financial risk internally, while still submitting claims to other payers. Thus, these organizational arrangements still involve transactions between provider and insurer organizations.

Managed care organizations also exchange administrative or clinical information internally and with their contract providers. In order to be profitable under flat-rate capitated contracts, managed care organizations must reduce duplicative services and manage each patient's utilization of services. This means that each clinician in the system who encounters a patient should ideally have access to a fairly complete medical record in order

BOX 3-2: What is a Value-Added Network?

Value-added networks (VANs) are the means most companies use to exchange electronic data interchange (EDI) transactions. VANs are the electronic equivalent of a package delivery service. Rather than make a direct computer connection with trading partners, companies send their data to a VAN. It receives a *bundle* of EDI transactions—representing many types of business documents and bound for many different trading partners—and routes the individual transactions to the appropriate trading partner's electronic mailbox. When the trading partner connects with the network, the EDI transactions are transmitted to its computer. VANs make EDI easier because they eliminate the scheduling problems that arise when making direct computer connections. They can also be more secure than direct computer connections because trading partners are isolated from each other's systems.

SOURCE: C. Canright, "Electronic Commerce and Networking in Health Care," unpublished contractor report prepared for the Office of Technology Assessment, U.S. Congress, Washington DC, Jan. 31, 1995.

to know what has been done by others. It also means that management should know what resources are expended on that patient, even when there is no need to actually generate a bill. Many managed care organizations are finding the need for "encounter reports" that contain much of the same information that is currently included in insurance claim forms in a fee-for-service system. While the encounter report could be considered an internal communication within the managed care company, in some cases delivering it will take very much the same technology and pose many of the same problems as the delivery of claim information between a provider and payer.

ADMINISTRATIVE ACTIVITIES IN HEALTH CARE

Administrative activities related to health care occur at all levels of the health care system, including health care providers, payers, and local, state, and federal government agencies. These activities include:

- *Health care providers (individual and institutional):* Calculating bills and billing payers; transmitting records to outside providers or payers; internal financial management; regulatory compliance; utilization review; quality assurance; and acquisition, distribution, and storage of equipment and supplies.
- *Payers:* Claims processing; coordinating benefits with other payers; claims payment; managing plan enrollment and eligibility; statistical analyses and quality assurance; and regulatory compliance.
- *Employers and other large purchasers of health care services:* Comparing and selecting plans; and managing enrollment of employees or members.
- *Consumers (patients):* Submitting claims; tracking eligible expenses; and paying copayments and uncovered bills.
- *Government agencies:* All of the above activities in roles as providers, payers, and employers; data collection for vital statistics; health care financing data; and regulatory oversight.

A fuller description of administrative activities and costs is available in a previous Office of Technology Assessment report, *International Comparisons of Administrative Costs in Health Care.*[5]

PROVIDER ADMINISTRATIVE ACTIVITIES

Many information exchanges that take place within a single provider's organization (e.g., admission-discharge-transfer messages or billing

[5] Office of Technology Assessment, op. cit., footnote 3.

information) are automated. Use of the Health Level 7 (HL7) standard, discussed in chapter 2, which is used for exchange of clinical information, is also growing for administrative and patient management information. Most vendors of both administrative and clinical information systems are supporting the HL7 standard. Use of computers in administration and patient management is not limited to hospitals or large clinics. Although many doctors' offices still rely on paper patient records and billing systems, a growing number are computerizing at least some of their business and administrative functions. Computerized practice management systems (PMSs) automate functions such as accounts receivable, insurance, billing, and appointments; they also record the patient's diagnoses, procedures, medical history, and financial history. PMSs offer a wide range of functionality and very little standardization; some systems were developed on an ad hoc basis by their users and others were purchased from one of more than 400 vendors. Some PMSs also help physicians deal with the complexities of managed care contracts, for example, by maintaining member lists, posting capitation payments from plans, tracking the number of visits or services provided for each patient, and providing reports on the profitability of the relationship with each plan.

Typically, providers only have information about their own contribution to a patient's care—for example, hospitals maintain records of inpatient stays and doctors' offices keep track of office visits. But to manage patients' use of resources effectively, managed care organizations want to track patient care over several years and integrate different services that were performed at various locations. Integration of financial and clinical information is also important to managed care.[6]

Integrated Delivery Systems (IDSs) are emerging to meet the need of health care organizations to deliver a full range of health care services to their covered populations. An IDS, either through ownership, partnership, joint venture, strategic alliance, or contract, brings together hospitals, ambulatory care facilities, affiliated physicians' offices, nursing homes, home care services, laboratories, wellness programs, and so on. IDSs have been springing up rapidly as managed care companies position themselves to compete; the result is a conglomeration of provider organizations with different levels and types of automation and uses of information technology. Some IDSs are making the investments needed to develop "enterprise-wide" information systems to allow exchange of clinical and administrative information among their various components.

Health care providers perform a variety of administrative activities associated with each admission, visit, or episode of care. These activities begin well before the face-to-face encounter with the patient and last long after the patient has left the institution or professional's office. Preadmission and preregistration cover a variety of logistical, clinical, and financial activities, including eligibility confirmations, certifications, and authorizations for care, which generally require communication with the patient's payer.

EXCHANGING INFORMATION BETWEEN PROVIDERS AND PAYERS

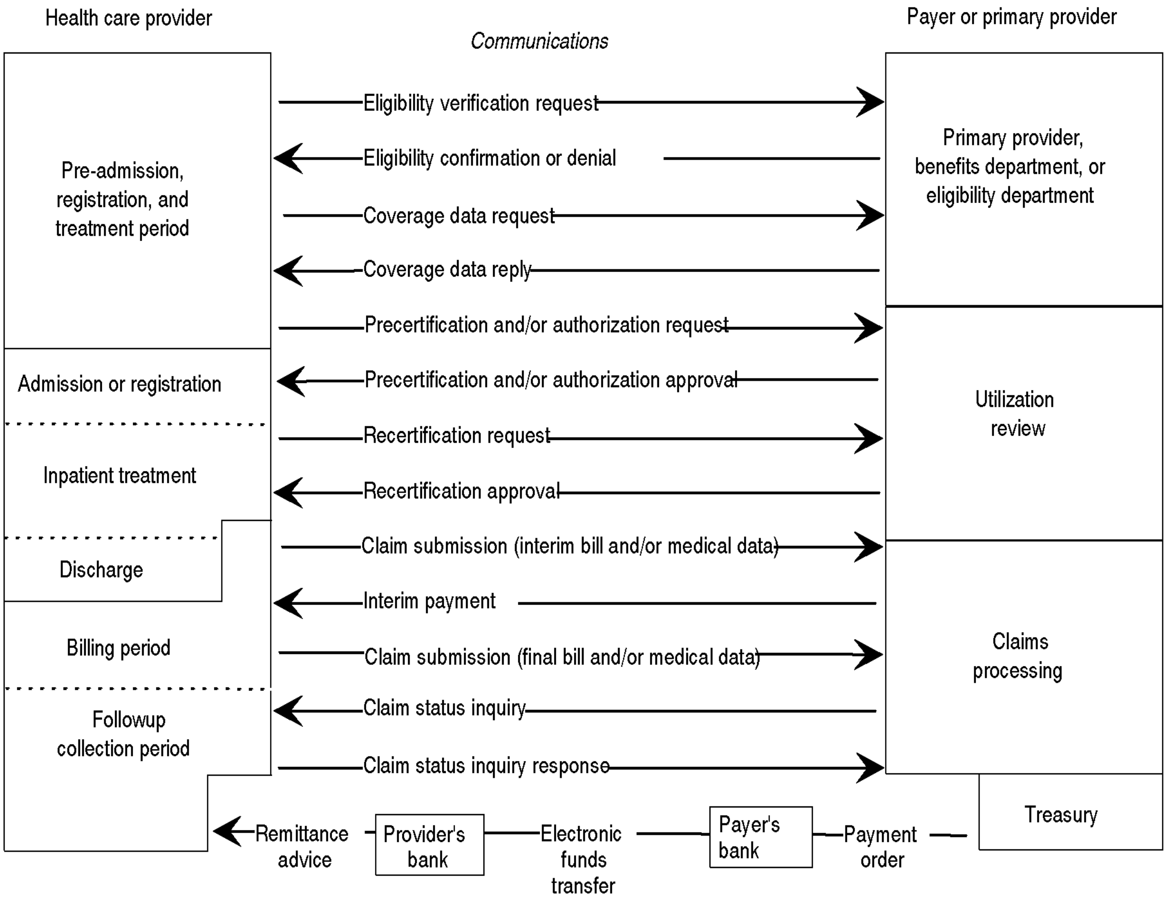
During the course of treatment or admission, additional transactions flow between the provider and payer or care manager, including reauthorizations, recertifications, interim billing, and a variety of review activities. Due to the limits on some health care coverage, the provider might also have to redo the eligibility function as well. Figure 3-2 illustrates some of the information flows between payer and provider at various stages in the process.[7]

At some point during or after treatment, the provider will issue a bill and/or a claim. Copies of the bill might go to the patient, as well as to one or

[6] D. S. Kolb and J. L. Horowitz, "Managing the Transition to Capitation," *Healthcare Financial Management,* February 1995.

[7] The following description of administrative information exchanges is based on information from D. Rode, immediate past co-chairman, ASC X12 Insurance Subcommittee, Healthcare Task Group, personal communication, May 12, 1995.

FIGURE 3-2: Payment-Related Transactions


Health care provider
Communications
Payer or primary provider
Pre-admission, registration, and treatment period
Admission or registration
Inpatient treatment
Discharge
Billing period
Followup collection period
Eligibility verification request
Eligibility confirmation or denial
Coverage data request
Coverage data reply
Precertification and/or authorization request
Precertification and/or authorization approval
Recertification request
Recertification approval
Claim submission (interim bill and/or medical data)
Interim payment
Claim submission (final bill and/or medical data)
Claim status inquiry
Claim status inquiry response
Primary provider, benefits department, or eligibility department
Utilization review
Claims processing
Treasury
Remittance advice
Provider's bank
Electronic funds transfer
Payer's bank
Payment order

SOURCE: Adapted from D. Rode, "EDI Holds Potential for Cutting Receivables Processing Costs," *Healthcare Financial Management Association*, March 1990, p. 15.

more payers. When more than one payer is involved, the provider may send a bill to all parties and work through a very complicated process to coordinate billing (and payment). Even patients who belong to managed care entities that capitate payments or use other reimbursement methods might need to have all or parts of their bill or claim sent for management information purposes.

After the initial claim or billing, the provider may have several followup steps, such as providing additional information to a payer inquiring about the status of a claim previously sent to one or more payers. Because more than one provider may be billing for services rendered during the same episode of care, both providers and payers may have to coordinate and track their information. Many institutions and some individual providers are also required to send additional information as attachments to the claim. Among the required documents are discharge abstracts, surgical reports, first reports of injury, and attestation reports. Late submission of these reports might also delay the payment of the original claim.

Finally, the provider receives a payment or rejection from the payer. This is a two-step process

QUANTITATIVE MEDICINE

Information systems allow many caregivers to share clinical and administrative information.

because the provider must reconcile the payment to the original claim, as well as to the posting process at its financial institution. The information received with the payment or rejection (usually called remittance advice) can be as simple as a check number or it may include pages of information responding to each line of the original claim. If the patient has health care coverage from a secondary payer, the provider may then have to repeat the process, submitting a secondary billing claim to that payer, and including with the claim information about what was and was not paid by the primary payer (some institutions bill the patient who is then responsible for collecting from secondary payers). On average, most institutions do not see payment on a claim for well over two months. Individual and professional payments often take longer.[8]

During the course of these provider-payer transactions there can be many telephone contacts and letters exchanged among the parties. In an inpatient environment, which is relatively stable, the cost of carrying out these transactions is relatively low compared to the amount of the claim. However, the opposite is true in an outpatient or ambulatory-care setting. The provider's costs for processing each transaction, claim, or eligibility verification is about the same as in an inpatient setting, but the resulting revenue is much less. The move of health care toward more outpatient care will accentuate this problem.

The traditional model for health payments has been that the provider charges the patient a fee for the services provided. The patient (or the provider on the patient's behalf) files a claim with the patient's insurer (payer) for payment of the covered portion of this fee. There are several types of transactions in the fee-for-service environment where electronic communications could be applied. These transactions are: 1) claims submission, 2) remittance advice, 3) claims inquiry, 4) enrollment, and 5) eligibility inquiry.

Claims submission is the process of preparing and submitting documents to a payer on behalf of a patient. Nearly all claims for hospital services are submitted by the provider. Claims for services in a physician's office may be prepared by either the patient or the provider; in preferred provider networks, the physician usually files the claim. Information required to complete the claim form may have entered the provider's accounting system through either a direct interface with other information systems in the provider organization, or through keyboard input by a data-entry clerk who reads the various paper documents about the patient and enters the data into the patient-accounting system. This system, whether paper-based or computer-based, must prepare a claim document in a form that is acceptable to the payer.

Remittance advice is a document returned to the provider by the payer along with payment after the claim is processed. The remittance advice explains what the payment covers and how the claim was adjudicated by the payer. The provider compares the payment with the original claim to determine whether the amounts match. If the claim and payment do not match, the clerk checks the remittance advice to determine where the differences lie. When the claim and the various payments match, either immediately or after a process

[8] A review of quarterly analyses by Zimmerman & Associates, Hales Corner, WI, shows receivables always exceed 60 days. Ibid.

of negotiating discrepancies, the claim is reconciled with its associated payments and closed. Remittance advice can be a paper document that accompanies a check; an electronic document that accompanies an electronic funds transfer; or an electronic document that is separate from, but related to, an electronic funds transfer sent by other means.

Claims inquiry is a process that providers use either to determine when payment will be made or to negotiate discrepancies in a claim that has been partially paid. Often, inquiries are telephone conversations, but some vendors are beginning to offer online inquiries.

Enrollment is a process that involves the payer and the patient's employer (or sponsor of the health care plan in which the patient enrolls). Enrollment transactions occur when people join a health plan, change their family status, move, change plans, and so on.

Eligibility inquiries are transactions between providers and payers to determine what benefits the patient is entitled to. Patients arriving at the doctor's office, hospital, pharmacy, or other provider location are asked what kind of coverage they have and from whom. This information is confirmed by an inquiry to the payer by mail, telephone call, or an electronic process. Having this confirmation quickly is useful to the provider: it means that correct copayment amounts can be collected right away, for example, or that certain services will not be offered to people who are not entitled to them. EDI standards have been developed for the above transactions. (See box 3-3.)

In a managed care environment, some of these transactions are different. For example, in an HMO, where members are charged a fixed fee per person (capitation) and are not billed for individual services, the traditional insurance claim is unnecessary. In some cases, however, HMOs are using an *encounter report* to provide management information about services provided, and these could be considered surrogates for insurance claims. Enrollment transactions and inquiries about a member's eligibility for services are as important in a managed care environment as in a fee-for-service system; in some cases, they may be internal transactions between parts of the same organization (perhaps at different locations) rather than between different organizations.

▮ Status of Electronic Insurance Transactions[9]

Health Care Financing Administration

As the largest payer of health care claims in the country, the federal government for years has encouraged providers and insurers to do business electronically, especially the submission of Medicare claims. The Medicare program (and the federal portion of the Medicaid program) is administered by the Health Care Financing Administration (HCFA) which, beginning in the 1970s, established electronic links between hospitals and fiscal intermediaries—the insurance companies that process Medicare claims under contract with the government. Currently, 80 different insurance companies process some 730 million Medicare claims annually.[10]

Initially, the shift away from paper involved hospitals submitting bills by either direct-data entry (DDE) terminal, linked directly by leased phone lines to the mainframe computer of the fiscal intermediary, or by computer tape. In either case, clerical personnel would key in the necessary information. For computer tape transactions, they would format the information on computer tape, which was then sent to the fiscal intermediary. For the fiscal intermediary, the volume of information received on tape—and thus the reduced costs of processing as compared with paper submissions—justified writing separate computer interfaces to translate the different tape formats as required.

[9] This section is based on C. Canright, "Electronic Commerce and Networking in Health Care," unpublished contractor report prepared for the Office of Technology Assessment, U.S. Congress, Washington, DC, January 1995.

[10] "Implementing EDI on a Colossal Scale: An Interview with HCFA's Carol Walton," *EDI Forum*, vol. 6, No. 2, 1993, p. 47.

BOX 3-3: EDI Standards

The key to the concept of *administrative simplification* lies in data standards. Standards are a theme throughout this report. Indeed, the one thing that nearly everyone involved in health care automation agrees on is that uniform data standards are required to control health care administration costs.

Roughly speaking, data-processing standards have two components: content and transmission. Data-content standards specify how meaning should be represented. Data-transmission (or messaging) standards specify how information encoded as strings of binary digits should be structured for transmission over wires or through the air.

Data Transmission

EDI standards for business documents structure information in such a way that computers at different organizations can process it. Computers do not process documents like humans read documents. Computers process data. To the computer, EDI is not a facsimile of a document that a computer stores; it is a stream of data that actually causes a computer application to perform a specific action.[1]

Data, however, are not quite enough. Data may be two-character codes that represent an idea or a string of characters that represent, for instance, a Social Security number (SSN). Because all data are represented as strings of 0s and 1s, computers need a means of distinguishing data denoting one idea from data denoting another.

Computers distinguish one bit of data from another through positional relationships. If a health care claim were written as a single line, then the computer would need to know what part of the line represented an SSN and what part represented a patient's name. By cutting that line of characters up into data elements, a computer can recognize one type of information from another. The first data element might represent a patient's name and address, while the second represents the line items on a claim. EDI standards provide that type of structure. They provide a common way for computers to structure the data that represent business documents.

The standards for moving the data that appear on common business documents between organizations are called the ASC X12 standards for electronic data interchange, named after the American National Standards Institute's Accredited Standards Committee X12, which develops them. ASC X12 standards define a syntax and provide a structure for moving data between organizations. In that way, EDI standards are external data-transmission standards. The structure that represents a business document is called a *transaction set*; transaction sets are the electronic equivalents of paper business documents.

Transaction sets, then, are composed of an ordered series of data segments. Data segments are analogous to the groups of data that perform specific functions within a business document, such as line items on a purchase order, terms of payment on an invoice, or the identification (name and address) sections that appear on any business document. Segments, in turn, are constructed of an ordered series of logically related data elements. Data elements specify such things as unit of measure, price, quantity, and currency.

Data Content

The content of standards comes to the fore at the data-element level of the X12 standards. Much of the content of a transaction set consists of codes used by a company or an industry to represent the

[1] E. J. Bass, "Introduction to EDI," unpublished paper presented to Accredited Standards Committee X12, St. Charles, IL, May 16, 1988.

(continued)

BOX 3-3: EDI Standards (Cont'd.)

specifics of its business. As much as possible, the X12 committee seeks to standardize content across industries. The segment and data elements used in transaction sets to represent a name and address, for instance, are the same for transportation concerns as for health care concerns.

Just because two organizations support the X12 standards, however, does not mean that communication between them is seamless. On a technical level, both systems are compatible because they are communicating using a common language. On a content level, however, compatibility is nowhere near guaranteed, particularly in health care. The data content of ASC X12 standards comes from industry- and company-specific codes. In health care, for instance, the ASC X12 health care remittance advice standard uses Adjustment Reason Codes maintained by the Blue Cross and Blue Shield Association and Current Procedural Terminology (CPT) Codes maintained by the American Medical Association. In fact, any organization can petition the ASC X12 committee to include its codes into the standard. As long as those codes meet the test of business necessity and perform functions that existing codes cannot perform, the codes are incorporated into the standard.

As a result, ASC X12 standards accommodate a huge amount of data content and they can perform the same business function in many different ways. Most industries have limited this variability by publishing implementation manuals specifying how a particular transaction set should be used to conduct business with companies in that industry.

The data content used in the ASC X12 health care transaction sets is still too broadly defined. Nearly everyone involved in EDI in the health care industry agrees that widespread EDI implementation will require greater uniformity in data content. As the WEDI committee puts it, "A significant barrier to the implementation of EDI is the fact that implementation guides have not been developed that incorporate standard requirements and content across large segments of the health care industry. It is critical that private payers and government programs, including Medicare and Medicaid, use a common set of formats to achieve the highest level of administrative cost savings and accelerate the implementation of EDI."[2]

The health care industry needs a business model that specifies the data required in each transaction and how they should be encoded and structured within the standards. Efficient standards require that all participants in the industry agree on: 1) what data to collect, 2) when to collect it, and 3) how to collect it.[3]

In the absence of industrywide implementation manuals, many in the industry are relying on implementation guidelines created by the Health Care Financing Administration (HCFA), the first payer to implement the health care claim payment and advice (ASC X12.835) transaction set and the claim submission (ASC X12.837) transaction set.

SOURCE: C. Canright, "Electronic Commerce and Networking in Health Care," unpublished contractor report prepared for the Office of Technology Assessment, Jan. 31, 1995.

[2] Workgroup for Electronic Data Interchange, *1993 Report* (Hartford, CT and Chicago, IL: October 1993), p. 1-7.

[3] G. Arges, Director, Health Data Management Group, American Hospital Association, interview, Chicago, IL, Aug. 25, 1994.

But as large chain-affiliated hospitals found that they were dealing with many different formats, they asked HCFA to establish a standard tape format, which it did in the late 1970s. The standard tape format allowed hospitals and other large institutions to introduce a degree of standardization into their claims submissions process. However, they still faced different data requirements from different fiscal intermediaries in different states.

During the 1980s, with the growing use of personal computers, HCFA also began to encourage physicians to do business electronically. In the mid-1980s, HCFA aggressively put pressure on providers to convert to electronic billing, and by 1985, HCFA received about two-thirds of Part A hospital claims and one-third of Part B supplemental insurance claims electronically.[11] Part A claims are submitted by hospitals and other large institutions for inpatient care. Part B claims are submitted by physicians and clinics.

HCFA's push for electronic claims processing came to a standstill in the late 1980s. Congress, as part of an attempt to balance the federal budget, mandated an extended timeframe for paying all Medicare claims. HCFA, however, had used expedited payment as an incentive for providers to submit bills electronically. Without the incentive of faster payment, many providers saw no reason to make the investments needed to submit claims electronically.

HCFA started to promote electronic billing again in 1991 as part of a short-term strategy to reduce administrative costs. Until then, HCFA had concerned itself solely with automating claims. In 1991, however, the agency turned its attention to automating the remittance advice document, which accompanies a claim payment and explains what the payment covers. Rather than develop its own remittance format, HCFA adopted the EDI format for health care remittance advices that had just been approved by Accredited Standards Committee X12. HCFA became the first organization to test the new EDI remittance advice format and remains its largest user.

In 1992, HCFA established a uniform payment policy and procedures for making electronic payments to medical providers for Medicare claims. Providers who submit at least 90 percent of their Medicare claims electronically can receive claims payments electronically through the banking industry's automated clearinghouse network and their local banks, rather than through paper checks mailed to their offices. HCFA again had a faster payment incentive to encourage electronic claims submissions. Since then, HCFA has adopted the EDI-based claims form as its standard and mandated that all Medicare processors adopt it by July 1, 1996. The agency's long-term goal is to have all Medicare claims handled electronically by the year 2000.

Private Insurers

Because many Medicare beneficiaries also carry private insurance policies that cover deductibles and copayment obligations under Medicare, HCFA's EDI projects also affect the administration of payments by private insurers. In many states, the fiscal intermediary for the Medicare program obtains its own private insurance claims electronically through the same linkages used for Medicare. With Medicare moving toward 100 percent electronic claim submission, "it seems likely that private firms will be making use of the technology as well."[12]

Some large insurers accept and process nearly 80 percent of claims by computer.[13] However, there are many small insurers that are only beginning to accept electronic claims. Today, about 75 percent of hospital claims are submitted electroni-

[11] M. Buffington, Director of Claims Processing, Health Care Financing Administration, personal communication, Sept. 7, 1994.

[12] D. Fularczyk, Manager, Blue Cross and Blue Shield United of Wisconsin's Proservices subsidiary, quoted in T. Higgins, "Setting Standard for Electronic Claims Could Lead to Paperless Providers," *The Business Journal-Milwaukee*, February 1993, pp. S3-S5.

[13] B. Politzer, "Claims of Excellence," *HMO Magazine*, vol. 32, No. 6, November-December 1991, p. 39.

cally, but the vast majority of these are Medicare claims submitted to HCFA rather than to private insurers. Physicians submit some 16 percent of their claims electronically in total; however, they submit 47 percent of their Medicare claims electronically.[14]

Electronic Medical Claims Services

One of the difficulties of connecting providers and payers is the different data and networking formats that exist in the health care industry. Conventional wisdom, for instance, holds that electronic claims are structured in some 400 different ways. Electronic medical claims companies, including value-added networks and clearinghouses, provide services that connect providers with many payers using a single system.[15]

These services give providers a single point of electronic contact to many payers. In addition to routing information between a provider and its payers, they edit and reformat claims data. This frees providers from the burden of programming their systems to handle the wide variety of electronic formats. For example, a physician's office wanting to send claims electronically generally uses personal computer software that communicates with the service via telephone lines. Physicians using practice management systems can often integrate this software with their systems. This requires that the processing service cooperate with the vendor of the practice management system (there are several hundred in the country) to write the necessary interfaces. For physicians who do not use practice management systems, the service provides software that allows clerical personnel to enter claims data directly into forms that appear on a PC screen.

Provider-specific edits are needed on each claim. Because health care claims are not universally standardized, different payers require data to be presented differently in their claims. One payer may also require data that another payer does not. The software checks the claims that are keyed in or received from a practice management system to make sure they conform to the data requirements of the designated payer.

If the claims meet all requirements, the PC software sends them to the electronic claims service. The service performs further editing and then transmits the claims to payers, in some cases through direct network connections to the payer and in others through a claims clearinghouse that has such a connection.

Many electronic medical claims services can perform some or all of the following transaction types: electronic claims filing; claims-status inquiry and online claims correction; eligibility and benefits inquiry; electronic remittance advice data; automated electronic remittance posting, along with supplemental and secondary billing; and electronic funds transfer. The services available to a provider vary by payer and depend on payer capabilities. Not all payers, for instance, can provide remittance advice data electronically.

Most of the transactions processed by electronic medical claims services are currently not based on EDI standards, particularly the nonclaims transactions. However, use of standard EDI claims may increase as HCFA mandates them. Until then, however, many payers are not accepting standard EDI claims. Nonclaims transactions, such as eligibility verification, are not based on EDI standards because the standards are either brand new or do not exist. Many of these services intend to support EDI standards, but place more emphasis on making transactions electronically, whatever the format. They believe that it is better to begin electronic processing now than to wait for the often slow standards-development cycle.

The initial cost of getting a physician started with an electronic claims service is between $1,500 and $2,500, depending on the size of the

[14] "Automated Medical Payments Statistical Overview," *Automated Medical Payments News*, Feb. 8, 1993, p. 3.

[15] B. Dodge, Vice President, HCS, Inc., personal communication, Aug. 26, 1994.

practice. Staff training may be an additional expense. There is also a per-transaction fee, which could be on the order of $0.35 to $0.85, depending on the type of transaction. Claims fall toward the upper end of the range because they are more complex documents and contain more data, while transactions such as eligibility inquiries cost less.[16]

In the early years of EDI development in other industries, value-added networks (VANs) offered similar translation services for companies that did not want to develop or install their own EDI management systems. Over time, companies purchased their own EDI systems, rather than pay translation fees to the VANs. A similar development is unlikely in health care. Only larger institutions are likely to have the financial and staff resources to manage an EDI system. For smaller medical practices, claims services and VANs may continue to provide a way to transact business electronically.

Financial Institutions

Completely automating the health care payment process means involving the trading partners' financial institutions. In the 1970s, the banking industry established its own formats for electronic funds transfer (EFT) through the National Automated Clearing House Association (NACHA). NACHA governs the automated clearinghouse (ACH), a network of computer-based check-clearing and settlement facilities for the interchange of electronic debits and credits among financial institutions (note that bank clearinghouses are different entities from the insurance clearinghouses mentioned above).

The banking industry designed its original EFT formats to move money between financial institutions. In the 1980s, NACHA worked with corporations to set ACH formats for corporate-to-corporate payments. At that point, the NACHA formats for EFT began to conflict with, and then migrate toward, industry's formats for EDI. The hybrid of EFT, whose purpose is to move money between financial institutions electronically, and EDI, whose purpose is to move business data between corporations electronically, became known as *financial EDI* (or EFT/EDI).

Since the development of financial EDI formats in the mid 1980s, the number of corporations using the ACH to make payments has steadily risen, showing an average annual growth of between 25 and 30 percent per year for the past several years. In terms of total payment volume, however, financial EDI volume statistics are less impressive. Last year, the estimated 13 million payments made through financial EDI represented only about 0.1 percent of the total estimated volume of 11.7 billion payments.[17]

Financial EDI payments, in all industries, consist of two parts: the payment and the remittance advice. One difficulty faced by the banking industry is that few banks are capable of processing all of the information contained in financial EDI payments. ACH formats themselves are not compatible with the information-laden EDI formats. To move *native* EDI data through the ACH requires *wrapping* an EDI transaction in a NACHA envelope. The financial institution then unwraps and processes the EDI payment transaction. The enveloping process puts some limitations on the amount of data an EDI transaction can carry—a potential problem given the amount of data in a health care remittance advice document.

As a result, many companies are sending EDI payment orders and remittance advices through separate paths—the payment itself as a simple EFT transfer through the ACH and the remittance advice as an EDI transmission through a VAN. In that case, companies receive the payment-deposit information from their banks and reconcile it with the remittance data received from the VAN.

However, some banks that specialize in financial EDI are moving into the health care market.

[16] Ibid.

[17] National Automated Clearing House Association figures reported in Canright, op. cit., footnote 9.

BankAmerica, San Francisco, CA; Chase Manhattan, New York, NY; Huntington Bancshares, Columbus, OH; PNC Bank Corp., Pittsburgh, PA; and National City Corp., Cleveland, OH, are among the national and regional banks that now process medical bill payments electronically for hospitals, clinics, and other health care providers who are their banking customers. Some of them, in addition to handling EFT payments, are also offering the services of a processing service.

▮ Standardized Forms

The federal government has played a major role in standardizing electronic forms in the health care industry. For instance, institutional providers are encouraged to submit Medicare and Medicaid claims using the UB-92 form, which was created by the National Uniform Billing Committee (NUBC). The difficulty is that each state adds its own requirements to the UB-92 form, which means that some payers and nearly all software vendors have to support nearly 50 different versions of the UB-92.[18] Moreover, the EDI standard for transmitting claims, ASC X12.837 (health care claim), can structure data contained in the UB-92 in several different ways, all of which are correct insofar as the standard is concerned.[19] The result is that the health care industry's standards are not yet standard enough for easy implementation of electronic commerce.

HCFA has developed implementation guides for health care claim and remittance advice transactions. By July 1, 1996, all electronic claims will be submitted to HCFA using the standard forms.[20] The HCFA requirement is expected to stimulate EDI use throughout the industry. To ensure that the health care industry uses a single EDI version of the UB-92, the Workgroup for Electronic Data Interchange (WEDI) and the NUBC are developing EDI implementation guidelines based on the HCFA guide, which is becoming the de facto industry standard.

LINKING HEALTH CARE PROVIDERS WITH SUPPLIERS[21]

In contrast with health care payments, the use of electronic commerce between large health care providers and hospital suppliers has a longer history, dating back to the mid-1970s when the American Hospital Supply Corp. (AHSC) introduced the first electronic order-entry (EOE) system called Analytic Systems Automated Purchasing (ASAP). ASAP initially allowed hospitals to place orders using a touch-tone telephone. As ASAP evolved, hospital purchasing managers could enter orders into terminals connected to AHSC's mainframe computer, which automatically reserved inventory and generated a packing list. The system was so convenient that purchasing managers placed orders with AHSC at the expense of its competitors.[22] Hospitals achieved benefits by: 1) eliminating manual order writing; 2) reducing transcription errors that result when orders are written manually or taken over the phone; and 3) increasing the accuracy and timeliness of order, delivery, and cost information.

The proliferation of other EOE systems became a problem to major hospitals, especially chains and large purchasing groups. Those organizations purchased supplies from several vendors, which meant they had to use several different EOE systems. They faced the same problems that have led to the development of EDI in other industries: higher costs from having to support multiple pro-

[18] D. Rode, "UB-92, HCFA 1500: The Genesis of EDI?" *Health Care Financial Management*, vol. 47, No. 1, January 1993, pp. 82-83.

[19] D. Hodges, *Integrating Computer-Based Technologies Into HMOs* (Washington, DC: Group Health Association of America, Inc., 1993), p. 41.

[20] M. Buffington, op. cit., footnote 11.

[21] This section is based on Canright, op. cit., footnote 9.

[22] R. Forester, "A History of ASAP at Baxter Health Care: The Journey from Proprietary to X12 Standards," *EDI Forum*, vol. 4, No. 1, 1991, p. 96. (Baxter acquired the ASAP system when it merged with American Hospital Supply Corp. in 1984.)

prietary systems,[23] including additional space for the terminals and additional training for purchasing personnel. Today, most hospital-supply companies are making a transition to EDI and offer EDI-based alternatives to their proprietary electronic order-entry systems.

In addition to the companies that directly supply hospitals and other providers, the companies that manufacture health care supplies and equipment are beginning to use EDI to connect with the smaller companies that they rely on to distribute their products to hospitals, physicians, and other health care providers. For the manufacturers, EDI connections result in cost savings because they no longer need to key purchasing information into their systems. By automating business with all their distributors, the relatively small benefits that come from automating each trading relationship are multiplied over a large base. For distributors, it is not clear whether the conversion to EDI results in net savings or net costs.

When the process of purchasing and paying for supplies is automated through EDI, it can be integrated with a larger automated materials management information system that can include inventory control, automatic replenishment, tracking of chargeable suppliers and equipment, invoicing, and patient cost accounting. Greater use of information systems for these purposes has been shown to improve inventory control and reduce the costs of materials management in other industries. Currently, only a few hospitals and health care groups are using this technology to its full potential.[24]

The movement to electronic systems in hospital materials management has not been pervasive among hospitals. By 1990, hospitals used EDI to place some 24 percent of orders to suppliers.[25] Purchase orders and confirmations still represent the bulk of EDI transactions in hospitals; hospitals have been slow to use EDI for other purchasing functions, such as electronic invoicing and payment.[26] WEDI, for instance, estimated that some 6,000 of 6,138 acute care hospitals require EDI upgrades.[27]

Overall, the health care supply portion of the health care industry has made a good start in automating trading relationships. As suppliers offer and providers adopt more sophisticated materials-management strategies, EDI will become increasingly necessary as well as commonplace.

PHARMACEUTICAL INDUSTRY EDI

The drug distribution chain has been an early and successful adopter of electronic commerce. As early as 1972, a major drug wholesaler began a pilot project to transmit purchase orders directly to the computers of major manufacturers. Industry organizations, such as the National Wholesale Druggists Association and the American Surgical Trade Association, actively supported these activities and encouraged the development of industry-wide standards. Use of electronic ordering was found to reduce order lead-times, which reduced inventory requirements. Some industry analysts believe that adopting electronic ordering is a major factor in alleviating and reversing economic

[23] The terms “proprietary system” and “proprietary data format” refer to electronic business communications systems that work for a single company—the one that provided the system or software. The terms “standard system” or “standard data format,” in contrast, refer to EDI systems that are designed to ease communications with any organization that supports EDI standards.

[24] ECRI, “Computer Information Systems, Materials Management,” *ECRI Special Reports*, 202765 424-008 (Butler Meeting, PA: 1995), p. 3.

[25] Arthur Andersen & Co., *Stockless Materials Management: How It Fits Into the Health Care Cost Puzzle* (Alexandria, VA: HIDA Educational Foundation, 1990), p. 56.

[26] J.J. Moynihan and K. Norman, “Health Care EDI: An Overview,” *EDI Forum,* vol. 6, No. 2, 1993, p. 11.

[27] Workgroup for Electronic Data Interchange, *Report* (Hartford, CT, and Chicago, IL: October 1993), p. 9-34.

hardships that drug wholesalers had been experiencing in the early 1980s.[28] By 1986, 96 percent of drug wholesalers were using EDI, as were 90 percent of pharmaceutical manufacturers—one of the highest penetration rates of any industry at that time.

Today, electronic commerce has also expanded rapidly to independent drugstores and drug chains. About 95 percent of drugstores are computerized. Many of them order from distributors using either proprietary systems or EDI standards and guidelines developed by the American Society of Automation in Pharmacy.

Because many prescription drugs are paid for or reimbursed by insurance plans, electronic links have also been established between pharmacies and payers. A standard format for communication between pharmacies and insurers is in widespread use. Online eligibility systems have helped to speed processing and payments by enabling pharmacies to check a patient's benefits before filling the prescription. After a physician or patient submits a prescription (either by phone or in writing), the pharmacy enters the information from the patient's prescription benefit card (issued by the insurer, health plan, or employer) and the information from the prescription into an online system using the National Counter Prescription Drug Plan's (NCPDP) standards for real-time transactions. Through this system, the pharmacy contacts a database where it can confirm the patient's eligibility status, find out whether the payer will pay for this drug, determine the copayment amount, and ascertain whether the payer allows or requires generic substitutions.

Pharmacy claims are much less complex than other health care claims, and a much larger percentage of them are submitted electronically. In 1993, over half of the prescription claims reimbursed by insurance payers were submitted electronically and that percentage continues to grow.[29] NCPDP recently introduced a paper-based claim form based on the electronic format to simplify reimbursement for patients whose payers are not yet using electronic pharmacy claim submission.[30]

The existence of large databases of prescription-related information in a standard format is offering new tools to both the pharmaceutical and insurance industries. Databases are being used to analyze the patterns of drug purchase, to develop formularies or lists of preferred drugs, to compare costs of alternative drugs, and to compare the cost-effectiveness of drugs to alternative treatments.

COMMUNITY AND REGIONAL NETWORKING

■ Community Health Information Networks

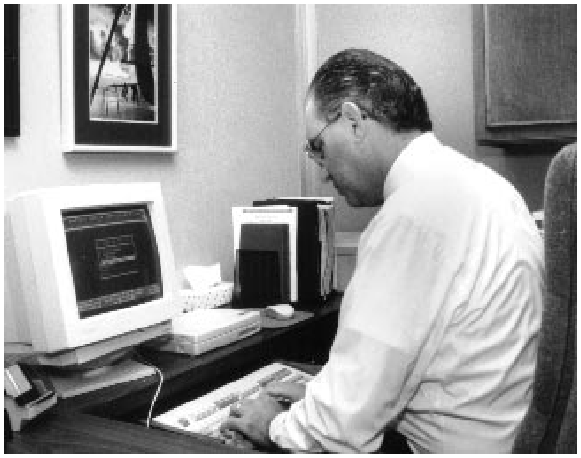
A *community health information network* (CHIN) can be either a proper or a generic name for a type of information system that is still undergoing development and definition. Another term used is *community health management information system* (CHMIS), which can also be both a common or proper name. Both of these networks are envisioned as systems that allow the seamless exchange of clinical or administrative information among health care providers, payers, and other authorized users. Currently, there are between 75 and 100 community networks in early stages of startup or implementation that roughly correspond to the CHIN or CHMIS descriptions below.[31] (This report will use the term CHIN as generic and will use CHMIS only when distinguishing features of the CHMIS model).

[28] P.K. Sokol, *From EDI to Electronic Commerce* (New York, NY: McGraw-Hill, Inc., 1995), pp. 212-219.

[29] Ibid.

[30] G. Muirhead, "Stake Your Rx Claim: NCPDP Issues Standard Paper Form for Reimbursement," *Drug Topics*, Nov. 7, 1994, p. 106.

[31] R. T. Wakerly, remarks at *CHINs and CHMISs: Networks for Community Health Information and Management*, meeting of the National Health Policy Forum, Washington, DC, Oct. 25, 1994.



SYSTEMS PLUS, INC.

Small clinics and individual health care providers are beginning to use computer-based systems for practice management, recordkeeping, and communication with laboratories, hospitals, and insurers.

At their most basic, CHINs are electronic systems whereby claims filing, eligibility verification, and other transactions can be performed by a provider (whether a single physician or a major health care organization) and an insurance clearinghouse; or whereby a physician's office can contact a hospital's information system to obtain clinical or administrative information on a patient. However, CHIN developers envision them as expanding into systems that link all participants in the health care system—providers, payers, banks, pharmacies, public health agencies, employers, and others. Moreover, a fully developed CHIN might allow a physician to assemble a single patient's information across different institutions and databases to produce a complete medical record; or it could permit a researcher to aggregate the data for many patients to compare performance of different plans and providers. In future, CHINs might also be a means for sharing access to medical knowledge, remote diagnostic applications, and expert advice based on outcome and effectiveness analyses.[32]

The difference between a CHIN and a CHMIS is primarily one of initial priorities. All of these systems start with some initial features and services and add others as they grow. CHINs, for the most part, were developed to provide connectivity and transport of data among the users. Some of them are concentrating first on linking physicians and clinics with hospitals and labs to access clinical data, and secondarily are providing claim filing and other insurance-related services. Some CHINs have a long-term goal of building a community-wide data repository for outcomes research and for comparing the performance of plans and providers, but they have not yet started that phase of their development. Other CHINs have no plans for building a centralized data repository, but envision that the standardization they provide will eventually allow authorized users to transparently aggregate data across many databases, thus accomplishing the same purpose.

CHMISs, on the other hand, have started with the concept of building a data repository for use in assessing the performance of health care providers and plans. Collection and analysis of management information is a priority. Although there is variation among the CHMISs started so far, most are focusing on providing insurance transaction services (that is, connectivity and services linking providers and payers) and on capturing data from those transactions into the data repository. Services linking providers with providers to exchange clinical data are also planned in many cases.

Issues associated with CHINs include ownership and control, and network design and data management.

Ownership and Control

There are several possible ownership models for CHINs. One is a joint venture between a health care provider and an information system vendor. This is likely to be a for-profit organization, offering community-wide service, with the goal of providing easier communications among the various

[32] D. L. Zimmerman, *CHINs and CHMISs: Networks for Community Health Information and Management.* Issue Brief No. 657 (Washington, DC: National Health Policy Forum, 1994).

users. The vendor may first implement services for the partner or lead sponsor and then attempt to contract with other users based on demonstrations of the usefulness of the service. An example of this ownership model is the Wisconsin Health Information Network (WHIN), developed by Aurora Health Care Corp. and Ameritech Health Connections (a subsidiary of Ameritech, the regional telephone provider). Initially, WHIN provided physicians with access to laboratory results, patient census data, and other information in the databases of the hospitals where they are affiliated. In addition, the network now offers an electronic claims service for filing claims and performing some other insurance transactions. Besides the Aurora-owned hospitals, 11 other hospitals and their affiliated physicians are now on the system. One difficulty with this ownership model is that the system may be viewed with some suspicion by competing hospitals who may worry that the provider that owns the system is giving itself some advantage. Even in cases where a vendor is sole owner, late adopters may view the system as "belonging" to the early adopters. There are 45 to 50 communities with vendor-owned CHINs.

An alternative model used by some CHINs is to form an understanding among a broad group of potential users before the system is built and create an ownership structure that will be viewed as more neutral by all participants. Although their organization varies, systems under development in Vermont, New York, Washington State, Chicago, Cincinnati, and other locations have attempted to develop a broad coalition of community groups—providers, payers, and employers—before the network is built. These groups then jointly sponsor the creation of a not-for-profit organization to operate the system. This model also has difficulties. Developing community consensus about the goals and operation of the system can take a great deal of time, so systems opting for this model come to market much more slowly. Agreements between stakeholder groups may become fragile when it becomes necessary for participants to actually commit money to the major project. It is not yet clear who should make the biggest investments in community networks because no one knows who will accrue the most benefit from them.

Other ownership patterns, including variations and hybrids of the above, ownership by a consortium of vendors, or ownership by a state or local government agency, are possible, and are being tried in some locations.[33]

■ Network Design and Data Management

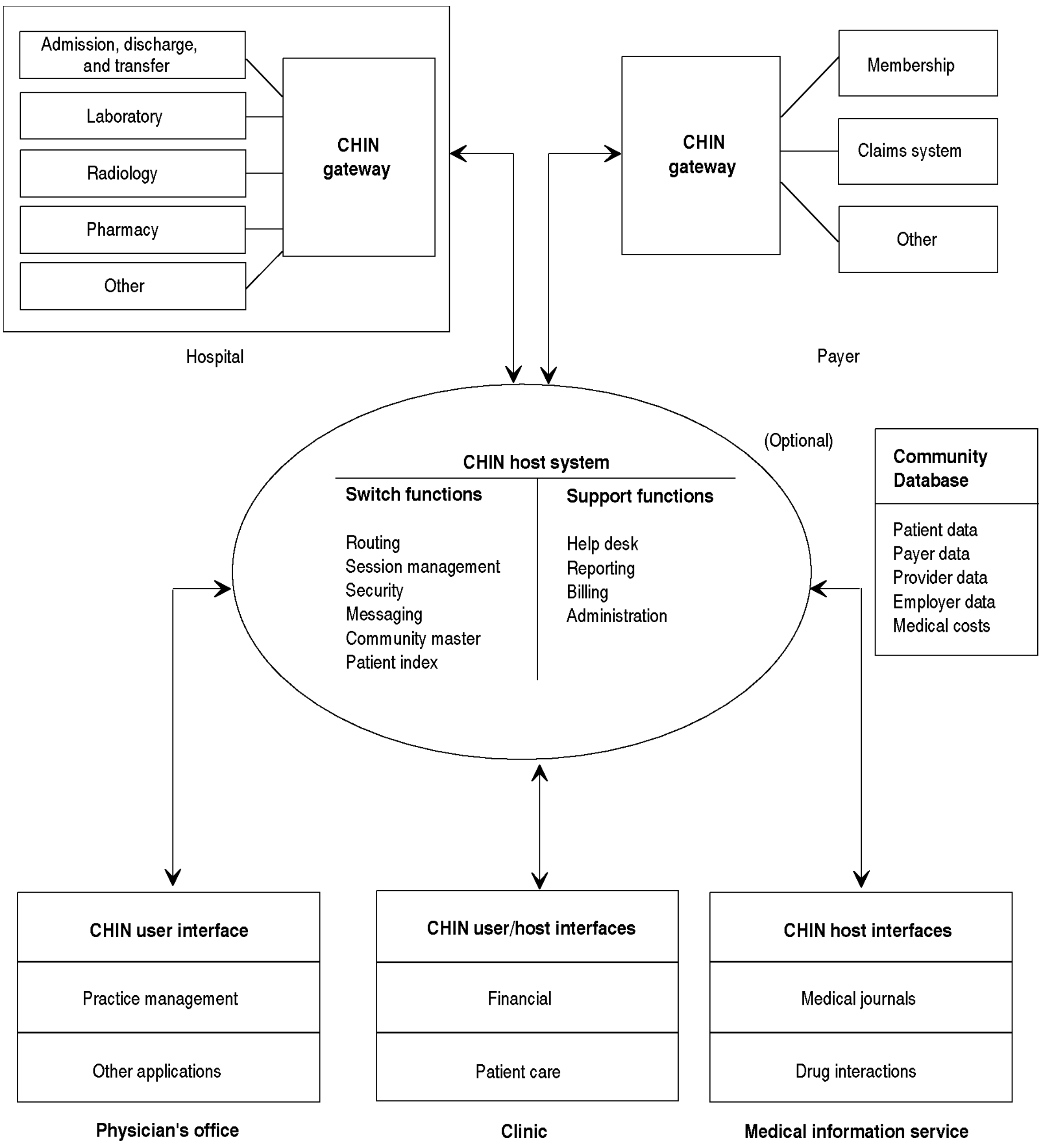
CHINs vary widely in their approach to the function of the network, the content of the information carried on it, and the standards to be used by or imposed on participants. One basic decision facing all CHINs is whether or not the network will maintain a central database of health information. Although creating a central repository is a fundamental goal of some networks, others have actively rejected the idea and use the fact that each participant maintains its own proprietary data as a selling point.

Technology decisions related to designing a CHIN are complex because their goal is to bring together a diverse set of information suppliers and users who are operating incompatible systems. The network must establish "rules of the road" so that participants can share information usefully. This means standardizing formats for data content and structure and creating interfaces so that different computers and different people can use them. In the absence of clear national standards, different CHINs are developing their own ways of doing this.

Figure 3-3 outlines the high-level architecture of a CHIN. The network must interact with a variety of different application systems in the participants' information systems. For the most part, network participants will not be willing or able to

[33] Ibid.

FIGURE 3-3: High-Level Architecture of a Community Health Information Network (CHIN)



SOURCE: M.R. Gorsage and J.W. Hoben, "Technological Implications of CHINs," in R.T. Wakerly (ed.), *Community Health Information Networks: Creating the Health Care Data Highway* (Chicago, IL: American Hospital Publishing, Inc., 1994), pp. 115-140.

change their own operations substantially in order to participate, so the network must develop interfaces to diverse systems as well as gateways (sometimes called application interface gateways or translators) to convert messages from one standard to another (e.g., from a proprietary system to HL7 or to a standard EDI format). The network provides a number of value-added services to participants, including switching functions like routing (delivering data between trading partners), security (maintaining passwords and access controls; encryption), session management (e.g., creating audit trails), and messaging (harmonizing disparate e-mail systems and providing access to external databases or networks). Generally the network also provides support functions for user organizations, including a help desk and billing and administrative information on system use.

User interface and point-of-service mechanisms, such as card readers and other devices, can provide access to the network and initiate transactions. For example, scanning a patient's identification card can initiate a verification of the patient's eligibility for benefits. For more information on cards as access and identification devices, see box 3-4.

User interfaces can be customized to allow each user to see data in the form that is most convenient for that user, as shown in figure 3-4. When a physician's office contacts different hospitals for patient information, the user will see the information in that office's preferred format, despite the differences in hospital information systems. Similarly, any data from the hospital that need to be downloaded into the physician's practice management system are formatted to be acceptable to that sys-

BOX 3-4: Card Technology and Health Records

Smart cards, magnetic stripe cards, and other small portable devices may offer a low-cost way to store and transfer electronic health information. Cards can be used as identification and authorization tools or as actual storage media. Cards currently play a role in the health care system, predominantly as a means of patient identification and association with a particular health plan.

Types of cards include:

- Paper cards, usually with printed data and perhaps with a bar code or magnetic stripe; these are usually issued by health plans as a means of identification.
- Magnetic stripe cards, such as those widely used in the financial industry (e.g., credit and automated teller machine—ATM—cards). The magnetic stripe on the back can carry a limited amount of information—226 characters in the case of a typical three-track card. They are typically used with online systems for accessing a database.
- Smart cards have an integrated circuit chip with a range of capabilities. They can support security features such as encryption and differential access for different parts of the card. They can be used to interact with online systems or to store varying amounts of data; the typical 24-kilobit card stores one full page of text. A backup copy of stored data may be kept on a provider's computer to protect against loss.
- Laser optical cards carry a wide stripe on the back that contains information that is "burned" into the card with a laser. Once written, data cannot be modified, although new data can be added to some types of laser optical cards. They can carry 2.5 megabytes of digital information (about 1,200 pages of text). They typically do not have security features unless an integrated circuit chip is added to the card for this purpose.

(continued)

BOX 3-4: Card Technology and Health Records (Cont'd.)

In the health care system, cards could be used to: streamline various administrative functions (e.g., claims processing); automate functions that tend to be repetitive in nature (e.g., filling out medical history forms); and improve the quality of care by reducing the likelihood of duplicative testing or possible drug interactions. Potential applications of card technology include:

- Patient Identification, enrollment verification, and eligibility verification
- Emergency Information
- Payments and claim processing
- Prescriptions
- Medical history

Magnetic stripe cards have wide use in health care in the United States, perhaps because of the large installed base of cards and card readers already in use by the financial industry and the public's familiarity with these cards. A number of U.S. health plans use plastic magnetic stripe cards, and at least 22 states use them to identify people eligible for Medicaid benefits. The patient presents the card when entering the hospital, provider's office, or other location. When the card is scanned, information that already exists about the patient can be linked with newly entered data in an automated fashion. Eligibility for service, the amount of the copayment, and other payment information can also be obtained quickly so that accounts can be settled before the patient leaves. Although magnetic stripe cards carry only a small amount of information, they are useful as access devices to link with the provider's or payer's online databases, and the U.S. telecommunications infrastructure is adequate to provide these linkages in almost any location.

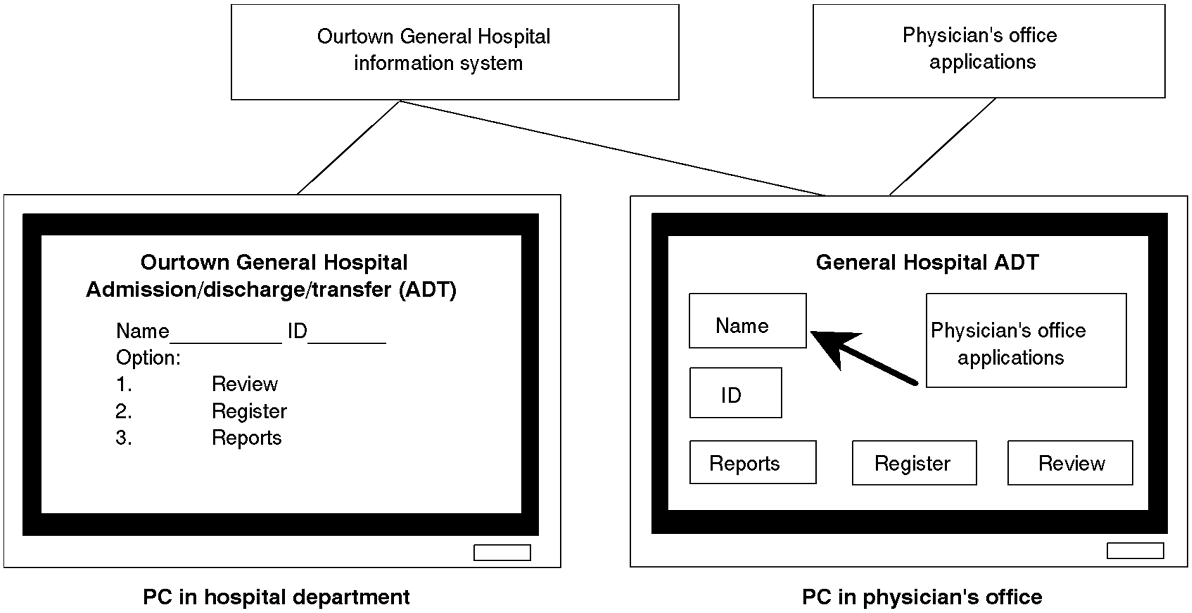
A number of health plans in the United States are testing the use of smart cards. Currently, standards for the data format, encryption, and security features are only beginning to emerge. This means that cards are only being used within closed systems. The Department of Defense is conducting a multimedia (magnetic stripe, bar code, integrated circuit chip, and photograph) identification card pilot program, which will test the viability of deploying smart cards for multifunctional purposes with a primary focus on health care. Canada, Great Britain, and Japan are also looking into smart cards for health care information.

Smart cards are used more widely in Europe than in the United States, but even in Europe, their use in health care is primarily for identification and for limited amounts of clinical and administrative information. In Germany, smart cards generally contain only administrative information. In France, cards typically contain some clinical information, but there is no attempt to store a complete medical record; rather, basic information is placed on the card and may be accessed by providers or pharmacies to reduce errors or to speed data processing. The storage capacity of many cards currently in use is usually not sufficient to maintain a complete medical history, although higher capacity cards are becoming available. Widespread use of portable electronic patient records in card form will depend on the availability of standardized patient record systems in the computers of all providers who will interact with and update the cards. Such systems are not currently available in Europe or the United States.

Laser optical cards are still an emerging technology and are not widely used. In one pilot project, the Texas Department of Human Resources has issued 2,500 cards containing demographic information and immunization records. Equipment to read the cards is available at only a few locations, but the project is expected to expand. Experiments with laser optical health cards are also under way in Scotland.

SOURCE: Adapted from Phoenix Planning and Evaluation, Ltd., "Potential Card Applications in the Health Care Industry," unpublished contractor report prepared for the Office of Technology Assessment, January 1994.

FIGURE 3-4: Common User Interface


Ourtown General Hospital information system
Physician's office applications
Ourtown General Hospital
Admission/discharge/transfer (ADT)
Name__________ ID_______
Option:
1. Review
2. Register
3. Reports
General Hospital ADT
Name
ID
Physician's office applications
Reports
Register
Review
PC in hospital department
PC in physician's office

Note: Common user system's sign-on allows for a custom screen (regardless of application) for users according to their profiles.

SOURCE: Adapted from M.R. Gorsage and J.W. Hoben, "Technological Implications of CHINs," in R.T. Wakerly (ed.), *Community Health Information Neworks: Creating the Health Care Data Highway* (Chicago, IL: American Hospital Publishing, Inc., 1994), pp. 115-140.

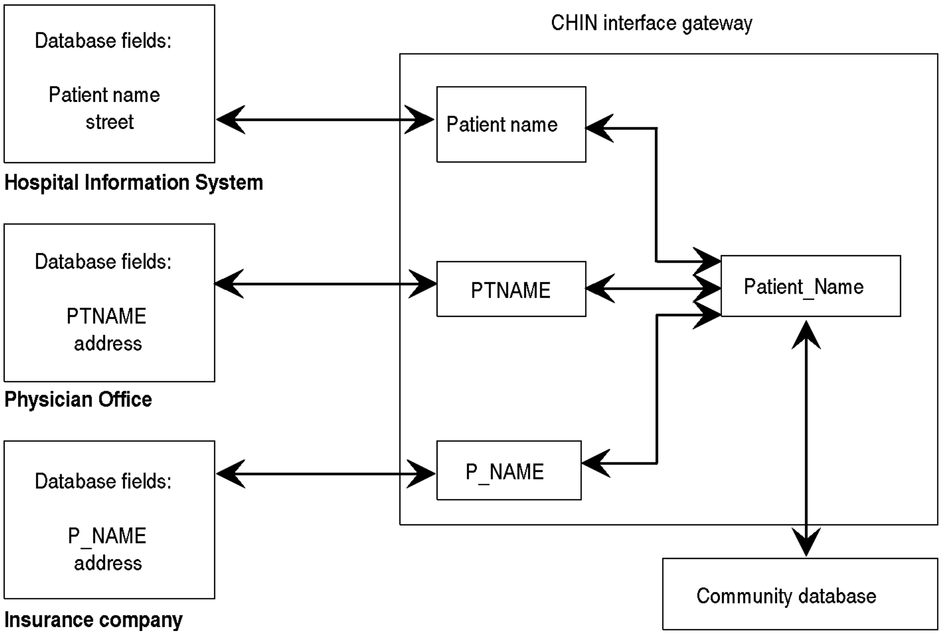
tem. The network system maintains a profile of each user and the way that information must be presented. Similarly, data for claims filing or other transactions can be entered by the physician's office in a single format, regardless of payer. The network, through the application integration gateway function, can then take responsibility for translating or reformatting the information to suit the requirements of each payer. This approach should reduce a participant's training costs because employees only have to learn one set of menus and navigational tools.

While the user's view of data appears integrated through the use of common user interface mechanisms, actually integrating data across multiple databases is another problem entirely. CHINs that include a central data repository are addressing this problem now. A repository is a "central database populated by transactions from several disparate departmental and organizational systems."[34] The repository contains *copies* of transaction data carried out by various trading partners; it is not the original or sole source of information. Management of information from disparate sources can be a complex task:

> To ensure data integrity, the [application integration gateway] should have data audit and control mechanisms to synchronize replicated data with its various storage locations. The task of determining which transaction system is the

[34] M.R. Gorsage and J.W. Hoben, "Technological Implications of CHINs," in R. T. Wakerly (ed.), *Community Health Information Networks: Creating the Health Care Data Highway* (Chicago, IL: American Hospital Publishing, Inc., 1994), pp. 115-140.

FIGURE 3-5: Federated Database Approach for a Community Health Information System (CHIN)



Note: Systems on the CHIN with their own repositories will require an intelligent gateway to match field names with data.

SOURCE: M.R. Gorsage and J.W. Hoben, "Technological Implications of CHINs," in R.T. Wakerly (ed.), *Community Health Information Neworks: Creating the Health Care Data Highway* (Chicago, IL: American Hospital Publishing, Inc., 1994), pp. 115-140.

master or owner of specific data elements is diplomatic and political rather than technological.[35]

Through use of a common data model, the repository can be mapped onto the various systems of record. Data for different entities can be tied together by using unique identifiers for patients, payers, sites, providers, and other entities.

In time, a central repository containing both clinical and administrative information could become too large to manage efficiently, especially if it includes diagnostic images. An alternative approach to managing community-wide information is to maintain an intelligent central repository that manages a federation of independent databases. All databases would share a common global model, and the central repository would contain not copies of the transactions, but information on where to find the information. This metatransaction (transactions about transactions) repository would then contact the individual databases to collect information needed by an authorized user, and would have the knowledge needed for resolving any differences between the databases. This concept is illustrated in figure 3-5.

Community Networks and Enterprise Networks

There is uncertainty about the role of CHINs as managed care organizations and integrated delivery systems (IDSs) begin to dominate health care

[35] Ibid.

delivery. CHIN development takes time and, in the meantime, some IDSs may build their own proprietary enterprise-wide networks. IDSs will carry out most of their data communication on their own enterprise networks because many of their administrative functions will be internal, and they may not need to join a community-wide network.

There are two schools of thought on the possible interactions of CHINs and IDS networks. One holds that IDSs have no need for CHINs, and that CHINs are a short-term or limited phenomenon that will fade as markets become dominated by two or three competing managed care organizations. Because the IDSs are competitors, they will have no incentive to share information, and thus connectivity between them will not be needed.

The other school of thought says that IDSs need CHINs because even in a managed care environment there will still be out-of-plan referrals, providers with multiple affiliations, and mobility of providers and patients among plans. In order to be totally electronic in processing administrative information, IDSs will need access to a community-wide or regional network infrastructure. Further, even though IDSs will want to keep private their own data on outcomes, utilization, and costs, it is likely that large purchasers of health care (and perhaps regulatory agencies) will insist on seeing at least some of this information on a community-wide basis, and CHINs will offer a mechanism.[36] There is even the view that some IDSs will eventually become CHINs, perhaps setting up subsidiaries to offer CHIN services to their competitors and unaffiliated providers in their communities.[37]

■ Networking and Public Health

The usefulness of community and regional networks increases if they are also able to interact with public health agencies at the local, state, or federal levels. The Department of Health and Human Services has been tasked by the Administration to act as the lead agency in coordinating federal government activities related to health information systems.[38] Among the long-term goals to be pursued is the creation of a national forum for collaboration on standards development for health information. Health information networks, automated payment systems, and other systems are part of the national information infrastructure (NII) where public- and private-sector activities need to be coordinated.

The Public Health Practice Program Office at the Centers for Disease Control (CDC) is developing an Information Network for Public Health Officials (INPHO) that provides state and local public health officials with access to timely information on disease prevention and health promotion, including: 1) local and national disease and injury rates and associated risk factors and prevention measures; 2) preventive health data, guidelines, regulations, training materials, and emergency notices; and 3) reports of epidemiological investigations. The system will initially employ CDC's personal computer software (WONDER) as well as voice and fax technologies, but will eventually use Internet tools. It will provide an electronic mail service for federal, state, and local public health officials, starting with local area networks and building toward wide area networks. The INPHO system is being pilot-tested in Georgia through a $5.2 million grant from the Robert W. Woodruff Foundation to Emory University in Atlanta, teamed with several other academic and state government organizations in Georgia.

COSTS AND COST-EFFECTIVENESS

■ System Costs

High system costs often pose a barrier for a business wanting to embrace EDI. Hardware, soft-

[36] F. Bazzoli, "Will CHINs Be Able To Mesh with Enterprise Networks?" *Health Data Management*, March 1995, pp. 47-52.

[37] R.T. Wakerly, "Models of CHIN Ownership," in Wakerly, op cit., footnote 34, pp. 53-71.

[38] A. Gore, Vice President, Washington, DC, memorandum to D. Shalala, Secretary of Health and Human Services, Washington, DC, Mar. 8, 1995.

ware, installation, and staff training are all expensive. If an organization opts to work through an electronic claims company or a VAN, it must pay per-transaction charges. If it creates a direct line to its trading partners, it will incur costs for network setup and telecommunications equipment. Staff will be required to manage the system, adapt it to changing standards, and act as a liaison with new trading partners.

One estimate puts the total average, per-company EDI investment at between $200,000 and $700,000.[39] The lower figure is for a supplier company, while the higher is for a large company seeking to connect all its suppliers. For the health care industry, WEDI estimates implementation costs at $7,500 to $15,000 for individual professionals and $25,000 to $500,000 for institutions.[40] Costs include hardware, software, consulting, and VAN charges. Most companies do not perform a break-even analysis, according to the EDI Group, a firm that studies EDI use generally. Those that do, however, report that they reach the break-even point within two years.[41]

There are relatively weak near-term incentives for some users in the health care industry to assume the high initial costs of EDI. Although there are promises of administrative savings, these will be spread out among most sectors of the industry. Further, it is likely that savings will not be fully realized until all transactions are electronic. A business that has some trading partners using EDI and some using paper has the expense of maintaining both systems. This is often the case in health care at this time.

National Estimates of Administrative Cost Savings

A number of key studies focus on national estimates of potential savings from using information technology for health care administrative functions. These include studies by WEDI, the Tiber Group, Arthur D. Little, Inc. (ADL), HCFA, and Lewin-VHI.[42] The findings of these studies are summarized in table 3-1. It is important to note that *comparisons across studies should be made with caution*: the definitions used for the various administrative transactions vary widely, as do the methodologies for estimating costs and savings. Still, it is instructive to examine the findings from these studies in clarifying possible savings from information technologies in health care.

The studies on national administrative savings project that information technology applications could save in the range of $5 billion to $36 billion per year in total health costs, which translates into approximately 0.5 to 3.6 percent of total national health spending. The Tiber Group study (which was commissioned as part of the WEDI Report) attempted to differentiate the savings per transaction for payers and for providers. It found that the greatest savings for both would be in the areas of claims inquiry and claims submission—which are very information-intensive. With the exception of the ADL report (which included some clinical as well as administrative functions), the magnitude of the projected annual savings was quite similar across studies.

There is some reason to believe that these estimates may be overly optimistic. For example, ex-

[39] D. M. Ferguson and D. J. Masson, “The State of EDI in the U.S. in 1993,” *EDI Forum*, vol. 6, No. 4, 1993, p. 10.

[40] R.L. Schaich, “Health Care Reform Costs and Benefits,” *EDI World*, vol. 3, No. 12, December 1993, p. 51.

[41] Ibid.

[42] WEDI estimates and Tiber Group estimates are reported in WEDI, op. cit., footnote 27; Arthur D. Little, Inc., *Telecommunications: Can It Help Solve America’s Health Care Problems?* No. 91810-98 (Cambridge, MA: July 1992); U.S. Department of Health and Human Services, Health Care Financing Administration, *White Paper on Financial Implications of Information Technology,* 1991; Lewin-VHI, *Reducing Administrative Costs in a Pluralistic Delivery System,* report prepared for the Healthcare Financial Management Association, Apr. 30, 1993).

TABLE 3-1: Estimates of Cost Savings for Payers, Providers, and Employers Through the Use of Information Technology

Study	Application/function	Claims submission	Enrollment	Payment & remittance	Eligibility	Claims inquiry	Total net savings
Workgroup for Electronic Data Interchange (WEDI)		$4.5 to $13.1 billion annually	$2.1 to $4.3 billion annually	$1.1 to $1.3 billion annually	$.25 to $ .49 billion annually	$.28 to $ .40 billion annually	$42 billion (over six years)
Key assumptions 1. A comprehensive, standardized Electronic Data Interchange capability is established throughout the health care system according to an aggressive implementation schedule over the next three years. 2. Standard formats will be adhered to very soon. 3. Employer automation costs only reflect the costs required to automate the transfer of enrollment data for companies with over 50 employees.		4. For enrollment, 171,722 employers with more than 50 employees will save 0 .5 to 1.0 FTE or $12,000 to $24,000 per year, minus annual transaction costs of $78 ($1.50 times 52 transactions). 5. For eligibility, there will be an elimination of nearly 6,000 institutions to maintain enrollment or eligibility lists supplied by payers 6. For payment and remittance, on average, there are 15 claims per remittance advice.			7. Implementation schedule assumes costs are amortized over three years - 30% implementation occurs in year 1 - 70% implementation occurs in year 2 - 100 % implementation occurs in year 3		
Sources: Previous WEDI findings, Health Care Financial Administration reports, A.D. Little report, Lewin-VHI report, proprietary data, and Tiber Group study, which was part of WEDI report.							
Tiber Group study		$0.73, $1.07	$0.64, $1.10	$0.19, $0.50	$0.98, $2.05	$2.72, $3.56	$24 billion
Key assumptions			(savings per transaction for insurer, then hospital)				(over 5 years)
1. Startup costs and fixed costs used in the study were assumed to be sufficient for 100% EDI. 2. Surveys were completed by only 14 physicians, nine hospitals, and six payers. Therefore, the data are assumed to be externally valid in order to project national savings.		3. Broad definitions for the applications (or transactions) were necessary due to definitional issues at many demonstration sites. 4. Even though price competition in the computer industry is quite high, costs were held constant for the study.					
Source: Surveys at each of three demonstration sites.							
Arthur D. Little		$6 billion annually					$36 billion annually
Key assumptions 1. The $30 billion in savings not due to claims submission will come from electronic management and transportation of patient information, including: the use of home health terminals to reduce discussions with providers; reduction in emergency room visits; early intervention; and improved creation, transport, storage, and retrieval of computer-based patient records. 2. Legal issues regarding liability will have been resolved.		3. Implementation costs are not included in the economic model.					
Sources: Data were gathered from available research and pilot studies when available; otherwise determined by panel of experts at Arthur D. Little.							

(continued)

TABLE 3-1: Estimates of Cost Savings for Payers, Providers, and Employers Through the Use of Information Technology (Cont'd.)

Study	Application/function	Claims submission	Enrollment	Payment & remittance	Eligibility	Claims inquiry	Total net savings
Health Care Financing Administration Key assumptions 1. For claims submission, payers and providers will each save 50 cents per claim for an estimated three billion paper claims. 2. For eligibility, assumed 75 million transactions and savings of $1.40 per transaction. 3. For claims inquiry, assumed provider savings would be one-half as much as payer savings estimated by WEDI 4. Administrative costs assumed to be growing at the rate of total health care expenditures. 5. Each visit, test, or procedure performed by a provider is counted as a separate "claim."		$5.8 billion annually	$0.4 billion annually	$2.4 billion annually	$0.8 billion annually	$0.1 billion annually	$43.6 to $74 billion (over six years)
Source: WEDI report provided most of the information.							
Lewin-VHI Key assumptions 1. The entire medical bill (all tests and procedures) is counted as one claim. 2. For claims submission, providers will save $1.30 per claim and payers will save 60 cents per claim.		$1.9 to $4.5 billion annually					$2.6 to $5.2 billion net in 1993
Sources: Cost estimates from Congressional Budget Office and General Accounting Office; industry sources, including The Medical Group Management Association; calculations by Lewin-VHI experts.							

SOURCE: Project HOPE Center for Health Affairs, Bethesda, MD, "Estimating the Cost-Effectiveness of Selected Information Technology Applications," unpublished contractor report prepared for the Office of Technology Assessment, U.S. Congress, Washington, DC, May 9, 1995.

perts interviewed by OTA note that the assumption by both WEDI and the Tiber Group that EDI will be rapidly implemented by a high percentage of providers and payers is unrealistic. However, the WEDI Report's other assumptions on savings from specific administrative transactions, which were based on industry surveys and case studies, seem to be more reasonable.[43] Potential savings noted in the ADL report also seem generous for a number of reasons. The report did not include the costs of implementing new systems, for example. The authors defended this omission by pointing to the variability of pricing, and the fact that the cost of implementation would be widely shared with other industry applications. Another problem was that some of the categories of cost savings were vague and the data used to support the claims were not always well justified. Finally, the results include some clinical applications as well as administrative applications, so comparisons with other national estimates are difficult to make.

The HCFA results, which relied heavily on the WEDI methodology, may also be optimistic for reasons noted above. In addition, the report was not explicit about how some of the calculations were made. The Lewin-VHI report was also vague about some of the assumptions underlying their calculations.

Despite limitations, however, it is interesting to note that the studies taken together suggest that information technology applications in health care administration will produce important, but not inordinate, savings to the health care system. In light of some claims made about the potential reduction in administrative costs that would arise from information technology, the actual savings projected appear rather modest. This general prediction seemed to be shared by experts interviewed by OTA. They also emphasized that the fact that existing studies do not show large savings does not diminish the potential importance of technology applications in increasing system efficiencies (which may be difficult to capture in an evaluation) or in improving patient care.

Savings from Reducing Errors and Detecting Fraud

Creating a health care bill or claim is a very complex process, and there are many opportunities for unintentional error or deliberate fraud. An important part of developing the bill is to describe the procedures performed for the patient. This information must be transferred from the patient record to the administrative system and, ultimately, into the bill or claim. Many payers, including HCFA, use one of several diagnostic and procedural coding languages, such as ICD-9-CM, as the basis of their payment formula. Many providers try to capture coding information as close to the source as possible, for example, by listing the code along with the procedure name on paper forms physicians use for ordering tests and procedures, or by having a computer-based system automatically record the code whenever a procedure is ordered by name. When diagnoses and procedures are not captured in coded form (e.g., if they are written in free-hand notes), then trained coders must read through the record to find information to be put in the bill.

The coding systems are far from perfect. Decisions about which code to use are not always clear and can be the subject of negotiation between payer and provider while a complex claim is adjudicated. Misreading, miskeying, and other mistakes can cause bills to have incorrect codes. In addition, some providers deliberately engage in fraudulent practices such as *upcoding* (describing the procedure performed with the code for a more complex one) and *unbundling* (billing for two or more procedures when a single comprehensive code exists that describes the procedure performed) in an attempt to get a higher level of compensation from the payer.

A number of software products have been developed to check claims for inconsistent, erro-

[43] Project HOPE Center for Health Affairs, op. cit., footnote 2.

neous, or suspicious coding. Some payers have their own proprietary systems to check claims before paying.[44] In addition, a number of commercial products are available for payers, providers, or other firms that prepare claims on a provider's behalf. Detecting obvious errors in bills saves providers the trouble and expense of submitting claims that will be rejected; such software is sometimes available in practice management systems and other administrative software for providers.

A recent study by the General Accounting Office (GAO) tested several commercial fraud-detecting software packages on samples of Medicare claims and found them very effective in detecting errors and flagging possible fraud. GAO suggested that use of such software could have saved HCFA about $603 million in 1993 and $640 million in 1994. These savings, amounting to about 1.8 percent of Medicare reimbursements for supplies and services, are in line with the savings reported by private insurers using the same software. GAO also notes that Medicare beneficiaries would have saved money as well—$134 million in 1993 and $142 million in 1994.[45]

Economic Justification of CHINs

No one has demonstrated whether of not CHINs are cost-effective. Those that exist have only been in operation for a few years and their data have not been publicly analyzed. However, the large investments made by vendors suggest that their own proprietary estimates show a profitable future for CHINs. On the other hand, a number of vendors have dropped out of this market already. In addition to the large investments involved, many of them have perceived the possibility, or experienced the reality, of failing to develop community consensus about the role of the CHIN and services that need to be provided. Even if a project is initiated by a vendor rather than a coalition of community groups, it is necessary to have the interest and commitment of a minimum number of potential customers from the relevant user groups; otherwise the project is too risky.[46]

The investment required to build a community network is large. Estimates for WHIN suggest that the partners invested $4 million to $6 million in hardware, software, sales, and operations teams before recouping any costs. Costs for WHIN subscribers depend on their size and the level of service they desire. A hospital might make a one-time investment of $50,000 to $125,000 (depending on its current level of automation, the number of custom interfaces that must be built, etc.). Ongoing costs are determined by an algorithm that includes the number of physicians on staff, number of beds, and annual patient visits. Other ongoing costs include a per-transaction cost for insurance transactions. Physicians' offices pay a $450 installation and training fee, an ongoing charge of $30 per physician per month, and a per-transaction charge for insurance services.[47]

Projected savings from participating in WHIN could be $750,000 to $1.5 million per year for a 300-bed hospital. The actual savings might depend on how effectively the hospital was using information technology and EDI before joining the community network. Before implementing the WHIN, the Aurora Health Care Corp. operated a proprietary network for communicating with physician offices. That system had required a $1 million initial investment and operating costs of $250,000 to $350,000 per year. Aurora estimates

[44] J. Newall and B. Colbert, "Using Automated Bundling, Unbundling, and Rebundling Processes Before Paying Claims," in *Health Information Networks,* proceedings of a conference sponsored by the Health Care and Insurance Institute, Sept. 28-29, 1993, Philadelphia, PA.

[45] U.S. Congress, General Accounting Office, *Medicare Claims: Commercial Technology Could Save Billions Lost to Billing Abuse,* GAO/IMD-95-135 (Washington, DC: May 1995).

[46] J. Sanders, remarks at *CHINs and CHMISs: Networks for Community Health Information and Management,* meeting of the National Health Policy Forum, Washington, DC, Oct. 25, 1994.

[47] M. Radaj, Vice President, Operations, Wisconsin Health Information Network, personal communication, July 8, 1994.

that participation in WHIN will provide greater functionality for half that cost per year. Annual savings for physicians' practices might be in the $2,500 to $5,000 range.[48] WHIN is currently working with the University of Wisconsin to conduct a cost-effectiveness study.

Cost savings to participants could accrue from a CHIN's ability to: 1) link participants; 2) deliver management information at the point of service; and 3) standardize electronic transactions. Linking participants electronically can reduce the need for telephone calls, travel, postage, and use of delivery services. For example, enabling physicians to check test results, sign attestations, or view images online presumably saves professional time by eliminating some trips to the hospital. Reducing phone calls can be difficult to quantify as a cost savings, but many office administrators have cited it as an immediate and welcome benefit of online systems.

Delivering management information at the point of service can facilitate the process of registering patients, checking their eligibility, and giving them care. Having management information available before treatment begins can reduce the number of rejected claims and other costs of working without complete information. In addition, user software at the provider's location can check the accuracy of entered data (e.g., in claim filing) and put data into a format preferred by the payer—all before it leaves the provider's premises. This could reduce personnel and staff training costs for both providers and payers, and reduce the costs of correcting rejected claims for both providers and payers. Of course, services like these do not necessarily have to be delivered over a community-wide network. A large number of insurance clearinghouses and other electronic medical claims services offer these services directly to providers. The possible advantage of a CHIN is to combine both clinical and insurance information processing in a single system

Community networks offer providers of all sizes the opportunity to move toward more uniform, standardized electronic communication without having the immediate need to change their existing systems. More information can be captured automatically and used in additional ways, which should reduce costs to participants. Use of common interfaces and elimination or standardization of some key entry tasks (such as filing insurance claims) could also reduce personnel and training costs.

POLICY IMPLICATIONS OF ELECTRONIC HEALTH INFORMATION

Among the issues affecting the health care industry's adoption of information technology are: 1) industry fragmentation; 2) complexity of information needs; 3) standards; 4) standard identifiers; 5) an inconsistent legislative and policy environment; and 6) privacy, confidentiality, and security concerns.

■ Industry Fragmentation[49]

The industries that have implemented electronic commerce most completely have been led by a single industry group devoted to implementing data standards. Examples include the Transportation Data Coordinating Committee that developed EDI standards for the transportation industry in the mid-1970s or the banking industry's National Automated Clearinghouse Association. The health care industry has no single focus for EDI activities. WEDI believes that implementation has been hampered as a result and will not proceed quickly unless a central entity is formed to coordinate implementation and education.[50]

An even more critical factor, however, is the fragmented nature of the health care industry in

[48] Ibid.

[49] This section is based on Canright, op. cit., footnote 9.

[50] Workgroup for Electronic Data Interchange, op. cit., footnote 27, p. 1-9.

general. In most industries where EDI has been successful (e.g., utilities, banking, transportation, and auto manufacturing), a few large organizations—called *hubs* in the language of electronic commerce—made EDI an explicit requirement for continuing a business relationship. Thus, for the smaller *spoke* companies, the decision was not whether to adopt EDI, but how quickly. One health care EDI consultant describes health care in the United States as a $900 billion "cottage industry."[51] There are over 1.2 million health care providers, ranging from single practitioners to 1,000-bed hospitals and more than 3,000 private payers. The effective number of different provider organizations may decline somewhat with the current trend toward hospital mergers, the purchase of clinics and medical practices by integrated delivery systems, and the continuing affiliation of physicians into independent practice associations and other arrangements. But the structure of the health care industry is unlikely to approach the relative simplicity of banking or air transportation. In health care, the industry hubs are providers, and most providers are small organizations without the time, finances, or staff resources to prepare implementation guidelines, set standards, and implement systems. They must rely on the guidance of vendors that provide software, claims processing, and networking services.

HCFA has been the successful organization in moving the health care industry toward EDI because of its financial reach. For many health care organizations, it was HCFA's development of the Medicare Transaction System (MTS) and its incentives to submit Medicare claims electronically that prompted initial interest in EDI. These incentives have included: 1) faster payment for clean claims (14 days for electronic, 27 for paper); 2) electronic funds transfer; and 3) free or at-cost billing software. Private sector payers are unlikely to offer many of these incentives to providers. For example, payers have an incentive to delay payment as long as possible in order to maximize their own use of the funds; they would be unlikely to offer providers quick payment as an incentive to begin an EDI relationship unless it could be clearly demonstrated that EDI reduces their own costs (not the provider's costs or the costs of the system as a whole) enough to offset this advantage. However, because many providers and payers are beginning to use EDI to deal with HCFA, the infrastructure is being created that they can also use to deal with one another.

Complexity of Information Needs

In banking and financial services, most electronic transactions are simple and highly standardized. Consumers and businesses benefit from the ease of using the automated teller machines and credit card transactions made possible by that standardization. Health care payment requires a number of different types of transactions, and often large amounts of data have to be exchanged. In addition, the procedures, information needs, payment arrangements, and authorization procedures for each type of transaction can vary, depending on the characteristics of the payer, patient, patient's employer, and sometimes the diagnosis or procedure involved.[52] This complexity has slowed the diffusion of electronic commerce into the health care arena.

Standards

The key to the functionality and growth of electronic medical payment lies in the establishment of standards. As discussed in chapter 2, standards-setting and acceptance are moving slowly. Current estimates put the number of proprietary claims formats in use at 400—too many even for software to translate between sender and receiver.

[51] J. J. Moynihan, "More Payers Should Convert to EDI," *Healthcare Financial Management,* vol. 48, No. 5, May 1994, p. 66.

[52] Faulkner and Gray Health Information Center, *Health Care and the Electronic Superhighway: A Provider Perspective on Electronic Data Interchange and Automated Medical Payment* (Washington, DC: Faulkner & Gray, 1992), p. 21.

The standards-setting process is voluntary and compliance with the standards will be voluntary as well. Yet administrative savings may not actually be realized unless standards are more stringent and compliance with them is nearly universal. As mentioned earlier, there are nearly 50 different implementations of the standard UB-92 form, requiring providers and payers with interstate business to use several versions of it. A standard claim form will not truly be standard, for example, as long as each payer can demand additional documentation to accompany it. While payers usually request additional information in an effort to reduce their own costs, the difficulty and expense of maintaining different forms presumably raises costs for the industry as a whole.

Standard Identifiers for Individuals, Providers, and Payers

Interstate electronic commerce for health information would be facilitated by a system of standard identifiers. Because each provider or provider group (as well as payers and other users of health information) maintains its own identification number scheme and assigns its own numbers, patient records are not uniquely identified once they leave the institutions where they have been created. This can create confusion in the multi-institutional sharing of clinical or administrative information. Unique identification can be accomplished by combining several different identifiers—for example, a file number, plus middle initial, plus address—but it is generally agreed that a system of standard identifiers would be more stable over time.

Some argue that the benefits of fully electronic records are more easily obtained if each individual could be uniquely identified. If each person had a universal patient identifier it would be easier to link the health information maintained at different institutions, for example. In addition to identifying patients, health care providers and specific sites of care also need to be identified. While there are a number of recommendations for developing numbering schemes de novo, some industry organizations recommend modifying or expanding existing identification number schemes in order to get unique identifiers in place more quickly.[53]

Universal identifiers are common in some European countries where they are assigned to people at birth. The United States has been slow to adopt a universal numbering system and many groups have actively opposed such a system based on privacy concerns.

The Social Security Number (SSN), or another number based on it, has been recommended for use as the universal patient identifier. Because this numbering system is already in place, some groups argue that it would be the fastest and least costly method of instituting a universal numbering system.[54] The ubiquity and convenience of the SSN make it a tempting candidate for a universal health identifier.

However, privacy advocates have opposed the use of the SSN as a health identifier precisely because it has had so many other uses. The SSN is the key to a lot of nonhealth-related information about a person—including financial, tax, credit, educational, and other information on file with government agencies and private firms. It is very easy, with access to the SSN, to quickly develop detailed dossiers on anyone. In addition, some individuals, primarily infants and noncitizens, do not have SSNs. Some people have multiple SSNs. The system has been in operation for 60 years, and there is a long history of invalid and fraudulently acquired numbers. Because the form of the SSN dates from the precomputer era, it also lacks a *check digit* (an extra digit added to a computer-based number that aids in error detection and correction).

[53] For example, see American Medical Informatics Association, "Position Paper on Standards for Medical Identifiers, Codes and Messages Needed To Create an Efficient Computer-Stored Medical Record" (Bethesda, MD: Apr. 20, 1993).

[54] Ibid., p. 2.

It can be argued that many of the privacy-based objections to the SSN—fraudulent numbers, linkages to other databases, and so on—will also apply to any new numbering scheme that could be adopted. While there is merit in this argument, there is also the possibility that a new numbering system would be safer because, for example, it would have legal protections from the outset to prevent its use for other purposes.

Alternative schemes for developing unique identifiers have been proposed. Some would include segments of the patient's name, latitude and longitude coordinates of the place of birth, date of birth, and perhaps parts of the SSN. Some systems also involve encrypting the number, or converting it to an alphanumeric identifier, in order to either protect privacy or to make the number shorter and easier to remember.[55]

One system that is now being put into place to identify providers is the National Provider Identifier (NPI), which will be implemented by HCFA in 1996. In its present form, the NPI system is not universal—it will apply only to Medicare participants. It will provide unique identification numbers for physicians, other providers, and the sites where they provide care. In developing the NPI system, HCFA worked with a number of federal, state, and private-sector organizations. The NPI will consist of a seven-character alphanumeric identifier with a one-character check digit. NPI numbers can be encrypted to protect privacy and confidentiality.

By design, there will be no *intelligence* imbedded in the NPI number; that is, analysis of the number itself will not yield useful information about the provider it identifies. Rather, the number points to a location in a database called the *National Provider File* that will contain descriptive data about the provider. Thus, numbers will not have to be reissued when provider characteristics (address, number of locations, or types of specialty) change. The numbering format has the potential to provide 10 million all-numeric identifiers or up to 27 billion alphanumeric identifiers, making it sufficiently large to serve as a national system for identifying all providers, including nonparticipants in Medicare. Should such a national system be desired, authorizing legislation would be needed to allow HCFA to open the system.

HCFA is also in the process of developing a registry and identifier system for payers. This system would identify and maintain information on the payers who offer secondary coverage for Medicare participants. The process of coordinating benefits is complex for Medicare as it is in the private sector. A primary payer, such as Medicare, is often not aware that a patient has secondary coverage, or may not have complete information on the benefits for which the patient is eligible and the rules for calculating reimbursement. Without this information, the primary payer can sometimes pay inappropriately (that is, pay more than the patient is entitled to). In addition, the process of filing a claim with the secondary payer is complex; the provider or patient must often file a separate claim based on remittance information provided by the primary payer. By incorporating a registry of secondary payers and a complete set of rules for coordination of benefits into its Medicare Transaction System, HCFA hopes to be able to more accurately calculate reimbursement based on all the benefits available to a patient. At the same time, it could automatically send a bill to the secondary payer, simplifying the claim process for patients and providers.

Inconsistent Regulatory Environment for Health Information

State government regulations concerning electronic health information and patient records, as well as privacy, vary widely. This creates a difficult environment in which to implement standard-

[55] For example, see P.C. Carpenter et al., "The Universal Patient Identifier: A Discussion and Proposal," *Patient Centered Computing: 17th Annual Symposium on Computer Applications in Medical Care* (New York, NY: McGraw Hill, Inc., 1993).

ized processes. There are four areas in which state legislation and regulation impact on electronic health information. They include laws on: 1) storage media for medical records; 2) use of electronic signatures; 3) privacy and confidentiality of health information; and 4) patient access to health records.

Storage Media for Medical Records

State governments generally have licensing authority over health care providers and require them to maintain medical records. Nearly every state regulates what media are permissible for storing medical records. In many states, the language is reasonably "technology neutral" and the use of catchall phrases such as "other useable forms" or "other appropriate processes" has been taken to mean that computerized record storage is permitted. In some states, however, legislation has served as a barrier to the development of automated patient records by specifying the permitted media (e.g., microfilm or paper) and excluding disks, tapes, and other computerized storage media. Other states require clinicians' signatures in ink on particular forms, implying a paper original to which the signature can be affixed. Some states specifically permit the use of computers for some functions but forbid it for others, thus hindering the development of a complete computer-based record. There are other paradoxes and inconsistencies in legislation as well, with some states permitting electronic signatures for some purposes but requiring retention of a paper or microfilmed record.[56]

Only a few states specifically authorize computerized medical records. Indiana statutes, for example, authorize the use of "computerized records that maintain confidentiality." They specifically state that the recording of hospital medical records by the data-processing system is "an original written record" and authorize the courts to treat information retrieved from such systems as originals for purposes of admissibility into evidence.[57]

Some of the states whose statutes posed barriers to electronic patient records are making progress toward changing the statutes. For example, North Dakota is considering legislation that would make the recording of a medical record on a computerized system the equivalent of a photographic process, thus making printouts and other items retrieved from the system admissible in court.

Recordkeeping rules for nonhospital providers—nursing homes and physicians' offices, for example—are often covered by different state statutes or regulations and can be very different from those that apply to hospitals in the same state. Implementing a complete electronic patient record in a multisite provider organization, that might include hospitals and nursing homes, can be complicated if these requirements differ widely.

The absence of state legislative or regulatory support for electronic patient records does not necessarily mean that providers in that state are forgoing development of information systems or electronic record systems. It does mean, however, that the providers face certain legal risks if they do not maintain the paper record system as well, and they must bear the costs of operating both systems. Currently, most providers are not technologically capable of creating a "complete" electronic record in any case. They maintain a mixed paper and electronic system for practical, as well as regulatory, reasons. The regulatory inconsistencies among states can create difficulties for health care organizations that are attempting to develop common patient record systems for sites in more than one state.

Federal legislation governing business records (which includes medical records) implies that computerized records are permitted (once again

[56] J. P. Tomes, *Compliance Guide to Electronic Health Records"* (New York, NY: Faulkner and Gray, 1994), pp. 14-19.

[57] Burns Ind. Code Ann. sec. 34-3-15.5-2.

using language about "other processes").[58] In addition, HCFA, which administers the Medicare program, authorizes the use of computerized medical records if they are maintained in a form that can be reproduced legally, and if the system meets Medicare's conditions for participation. These conditions basically state that the system must protect the security of the records and ensure that only the authorized persons are able to sign them. The Department of Health and Human Services, in an effort to encourage the development of computerized patient records, had legislation introduced in the 103d Congress to require providers to maintain outpatient data in electronic form as a condition of participation in Medicare.[59]

Electronic Signatures

Signatures are necessary to attest to the completeness and authenticity of a medical record. Generally, each entry in a record is signed or authenticated by the person responsible for that entry. An electronic record can be signed electronically, and this is permitted in many states; once again, however, electronic signatures are treated differently from state to state. Some states are silent about the specific means or technology to be used for the signature, or they say that industry and professional standards should dictate the form of the signature. This would seem to permit the use of electronic signatures in those states because the Joint Commission on Accreditation of Healthcare Organizations, American Hospital Association, and other industry groups have published guidelines related to electronic signatures. Some states (like Pennsylvania, Alaska, and California) specifically authorize the use of an electronic signature activated by a computer key that is known only to the authorized user.

HCFA accepts electronic signatures on admission data sheets, attestations, and other documents used to reimburse providers treating Medicare patients. Providers must demonstrate that their computer systems meet HCFA guidelines.

Privacy and Confidentiality of Health Information

Both federal and state legislation cover the privacy of patient records. Records held by the federal government are protected under the Privacy Act,[60] which governs federal disclosure of confidential information. At the state level there is a variety of approaches to privacy protection, and a number of states have privacy laws that cover medical information. Other states have sections in their Medical Practice Acts that prohibit physicians from revealing information obtained in confidence from a patient during treatment. The American Medical Association has published standards for hospitals to protect the privacy of patient information. Some courts have enforced these standards under state contract law as implied conditions of the contractual relationship between physicians and patients.

Even among the states that have well-defined laws on the privacy of medical records, few address the flow of information to secondary users, such as insurance payers, researchers, and so forth. Further, because states are so inconsistent in how they deal with electronic information generally, few of them confront issues directly related to protecting privacy in *computerized* patient records. For a more detailed discussion, see the previous OTA report, *Protecting Privacy in Computerized Medical Information.*[61]

[58] 28 U.S.C. 1732.

[59] Tomes, op. cit., footnote 56, p. 14.

[60] 5 U.S.C. sec. 552a.

[61] U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993), pp. 41-45.

Patient Access to Health Records

Because patients have a property right in their records, it seems reasonable that they should be able to inspect or copy them. Access to medical records held by the federal government (e.g., Department of Veterans Affairs or other hospitals operated by the federal government) is governed by the Privacy Act. The Privacy Act requires agencies to establish procedures under which individuals can view or receive copies of their own records. It also authorizes the establishment of special procedures for handling information that might, in the judgment of the agency, have an adverse effect on the individual. These procedures have generally involved designating a third party to examine the records and releasing them to a physician designated by the patient.[62]

For private sector hospitals and other providers, state laws and regulations govern patient access to medical records. Thirty-seven states have statutory provisions for allowing a patient to review and/or copy his or her medical records. In a few additional states, the patient's right to access is not specifically stated, but can be inferred from other language.[63] In addition, some courts have ruled that providers have a common-law duty to allow a patient to access his or her records, absent legislation.[64] In 22 states, the patient may be charged reasonable copying fees, and 19 require that the patient apply for the records in writing. Twelve states permit physicians to deny patient access to a record if something in the record would have an adverse affect on the patient; in most of these cases, however, the record must be released to an attorney, physician, or other representative designated by the patient.[65]

A patient's right of access to information derived from the medical record, but housed in the database of an insurer or other third party, is unclear in many states. Only 14 states have legislation giving patients access to insurance databases and limiting redisclosure of medical information held by nonproviders.[66]

Privacy, Confidentiality, and Security of Health Information

Privacy, confidentiality, and security of electronic data are areas of great concern because of the sensitivity of health information. *Privacy* is essentially the right of an individual to limit access to information regarding that individual. *Confidentiality* is a form of informational privacy characterized by a special relationship between people, such as the relationship between doctor and patient. *Security* refers to technical and organizational procedures that protect electronic information and data-processing systems from unauthorized access, modification, destruction, or misuse.[67]

The appropriate levels of privacy, confidentiality, and security, as well as the techniques for achieving them, may vary depending on the institutional context and the use of the information. Tradeoffs are often necessary. For example, within a single hospital, confidentiality might be best served by allowing a patient's record to be seen

[62] U.S. Congress, Congressional Research Service, *Access to Medical Records Under Federal Law*, No. 93-708A (Washington, DC: Aug. 3, 1993), p. 16.

[63] U.S. Congress, Congressional Research Service, *Patient Access to Medical Records: A Statutory Survey of the United States*, No. 92-896A (Washington, DC: Nov. 17, 1992), and *Medical Records: State Laws and Regulations Regarding Ownership and Patient Access*, No. 93-519A (Washington, DC: May 20, 1993).

[64] R. S. Dick and E.B. Steen (eds.), *The Computer-Based Patient Record: An Essential Technology for Health Care* (Washington, DC: National Academy Press, 1991), p. 166.

[65] U.S., Congressional Research Service, *Patient Access,* op. cit., footnote 63.

[66] Dick and Steen, op. cit., footnote 64.

[67] L. O. Gostin et al., "Privacy and Security of Personal Information in a New Health Care System," *The Journal of the American Medical Association*, vol. 270, No. 20, Nov. 24, 1993, p. 2487.

only by the attending physician and the nurse assigned to that patient. However, such a policy would affect the quality of patient care—it would unduly inconvenience and slow the work of substitute nurses, consulting physicians, intensive care personnel, or other caregivers who might need the record on short notice. Thus, a balance between confidentiality and convenience must be found. Most hospitals allow fairly broad access to patient records by authorized caregivers, and they usually have security systems to keep track of each access. In some cases, this feature is used regularly to keep caregivers aware that they are accountable for their use of the information system. At one hospital, for example, users are regularly notified on-screen that each instance of access to a patient record is automatically recorded and that patients have the right to see a list of those who looked at their records.[68]

When information moves out of the single provider institution, priorities may change. The EDI industry has focused most of its concern on the security of information. Companies engaged in transmitting business information electronically—financial institutions in particular—have adopted technical solutions to two problems. The first is that information transmitted over phone lines might be read by unauthorized persons. One technique for addressing this is *encryption*. A second problem is that people sending or receiving information may not, in fact, be who they say they are. *Authentication* techniques—the use of passwords, keys, and other automated identifiers—are used to verify the identity of the person sending or receiving information.[69]

Thus far, the EDI industry has a good security record, according to the Workgroup on Electronic Data Interchange (WEDI), which says "there have been no reported incidents of the confidentiality of EDI messages being compromised."[70] Indeed, the risk of data leakage to outside computer hackers can be minimized in an online system. Security measures such as encryption procedures, password access, and audit logs help to discourage data theft. With electronic information, system administrators have more numerous and powerful tools for monitoring and protecting information than they do with paper-based records.[71]

Privacy and confidentiality—the main focus of concern for the health care industry—are proving more difficult to protect. As health care information increasingly moves over electronic networks, it becomes accessible to more people at widely scattered institutions with different policies and procedures in place. The potential for abuse increases accordingly. Unauthorized uses of information by authorized users can be a major problem that is difficult to stop by technological means. Because of a plethora of conflicting state laws regarding confidentiality, it is difficult to establish legally defensible policies on proper access to records; people handling records often have no clear guidelines for acceptable release of information. A 1993 OTA report on privacy and confidentiality of health information notes:

> The present system of protection for health care information offers a patchwork of codes; State laws of varying scope; and Federal laws applicable to only limited kinds of information, or information maintained specifically by the

[68] C. Safran et al., "Protection of Confidentiality in the Computer-Based Patient Record," *M.D. Computing,* vol. 12, No. 3, 1995.

[69] For further information on network security issues and technologies, see U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994) and *Issue Update On Information Security and Privacy in Network Environments,* OTA-BP-TCT-147 (Washington, DC: Government Printing Office, June 1995).

[70] Quoted in Benjamin Wright, "Health Care and Privacy Law in Electronic Commerce," *Health Care Financial Management,* vol. 48, No. 1, January 1994.

[71] Ibid.

> Federal Government. The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment.[72]

The situation has not changed appreciably since this report was published.

Without uniform privacy and confidentiality laws, it is extremely difficult to expedite the development of interstate health records transfer. Accordingly, WEDI called on Congress to ensure the uniform, confidential treatment of identifiable information in electronic environments. As electronic interstate transfer of medical data increases, policies concerning the access to medical information by secondary users of medical data, the use of medical data for nontreatment purposes, and the redress of privacy violations must be made consistent in all state. Privacy legislation should also address the requirements for informed consent of patients. Patients are often unaware of how their medical information will be used, to whom it may be released, and what rights they may have to access or correct it once it is in the hands of a secondary user.

Whether information is stored in a computer or on a piece of paper, the public fears the abuse of medical information by both authorized and unauthorized parties. In a 1993 health privacy poll, 80 percent of all respondents believed that consumers had lost all control over the circulation and use of health care information.[73] These concerns can lead (and have led) to physicians withholding information from patient records at the patient's request in order to protect his or her privacy.[74] To create an inaccurate or incomplete patient record, even with beneficial intent, could ultimately have serious effects on the patient; in addition, such actions render records less useful for outcomes research and other statistical purposes.

Improved patient education about privacy rights may decrease the lack of control patients feel over the spread of medical information. Until national, uniform privacy legislation is enacted, WEDI suggests steps to protect privacy in its 1992 report.[75] Providers should:

- ensure that the patient has authorized release of health information to an insurer by signing the release contained on the insurance form,
- ensure that they release information in strict compliance with the written release,
- ensure that they have complied with any relevant laws governing disclosure to insurers,
- establish security policies for employees who have access to and process patient health information, and
- establish security protocols for computer systems used to process claims.

The WEDI guidelines were not intended to replace the need for federal legislation or to absolve system operators from responsibility to design and maintain secure computing environments.

Although solutions to the networking problems of privacy, confidentiality, and security remain unclear, the questions they embody do not: What potential benefits of increased access to health care information will materialize, and will they outweigh the reduction in individual privacy that increased access to information inevitably brings? These questions must receive considered answers. "Opportunities for using electronic networks may be lost if there is serious mistrust of their safety."[76]

The concept of *fair information practices* set forth in the federal Privacy Act is fundamental to a number of existing privacy laws and proposed ini-

[72] Office of Technology Assessment, op. cit., footnote 60, p. 13.

[73] Gostin et al., op. cit., footnote 67.

[74] Office of Technology Assessment, op. cit., footnote 60, p. 6.

[75] Workgroup for Electronic Data Interchange, *1992 Report* (Hartford, CT, and Chicago, IL: September 1992).

[76] Gostin et al., op. cit., footnote 67.

tiatives to protect medical information. Common characteristics are:

1. Records pertain to medical information on individuals.
2. Individuals are given the right to access much of the personal information kept on them.
3. Limits are placed on the disclosure of certain personal information to third parties.
4. Health care personnel are required to request information directly from the individual to whom it pertains, whenever possible.
5. When a government entity requests personal information from an individual, laws require the individual to be notified of the authority for the collection of data, whether the disclosure is mandatory or voluntary.
6. The individual may contest the accuracy, completeness, and timeliness of his or her personal information and request an amendment.
7. Health care personnel must decide whether to amend the information within a fixed time, usually 30 days after receiving a request.
8. The individual whose request for change is denied may file a statement of disagreement, which must be included in the record and disclosed along with it thereafter.
9. The individual can seek review of a denied request.

Protecting Privacy in Computerized Medical Records[77] noted that basing new protection for medical information solely on the Privacy Act and on principles of fair information practices will fail to consider the complexity of today's information environment, with its distributed processing, sophisticated database management systems, computer networks, and widespread use of microcomputers.

> It is apparent that protecting personal information in a computerized environment involves, at a minimum, access to records, security of information flows, and new methods of informing individuals where information is stored, where it has been sent, and how it is being used.[78]

POLICY CONSIDERATIONS FOR CONGRESS

Attempts to improve administrative efficiency by increased use of electronic commerce in health care are an important component of a larger effort to reduce costs, improve quality of care, and improve access. Compared with a paper-based system, electronic information systems do appear to reduce costs for some users. The industry is moving in this direction. Standards development activities are under way.

However, getting started with electronic commerce is expensive. Some organizations have weak financial incentives to make the necessary investments to institute electronic payments, while others are forging ahead without waiting for standards to be set. Some experts interviewed by OTA commented that the complexities of dealing with paper records and paper-based transactions, particularly as health care organizations grow larger and enter new lines of business, are forcing some organizations to implement electronic systems, even if they have no way to measure the actual cost-effectiveness of a particular system. The computer network, like the telephone, is becoming a part of the way business is conducted; a firm simply has to have one to compete in the market, whether it makes economic sense or not.[79]

There may be some savings for the health care system as a whole if electronic medical payments, for example, are implemented on a near-universal scale. However, at current rates of implementation, high levels of use of electronic payments or compliance with standards may not be achieved for some time. The health care industry in the

[77] Office of Technology Assessment, op. cit., footnote 60.

[78] Ibid., p. 79.

[79] Project HOPE Center for Health Affairs, op. cit., footnote 2.

United States is not organized as a "system" with a central focus or consensus on how to deal with systemwide problems. The different parts of the system have diverse incentives, and efforts to control costs in one area may increase costs in another. However, these shifted costs are so subtle and spread over so many participants in a complex system that they are hard to quantify. For example, a major payer, in an effort to reduce its own costs, may begin to request additional data and documentation (beyond what is on the standard forms) when providers submit large claims. All providers who deal with that payer then incur additional costs to resubmit rejected claims, develop and maintain different versions of the standard form, or provide the additional data with all claims to avoid the problem of deciding when to send it and when not to. Situations like these make it difficult for the industry to establish truly uniform procedures.

The trend toward managed care reduces this diversity of interest to some extent. The percentage of people covered by traditional indemnity insurance in the fee-for-service sector can be expected to decrease, thus reducing the number of transactions between providers and payers as well. Some managed care organizations, like staff model HMOs, will internalize these transactions, and will presumably perform them efficiently out of sheer corporate self-interest. But managed care is taking many forms, including independent practice associations and other arrangements for which transactions will remain external between a network of different provider and payer organizations. For the near future, absent a far-reaching government-imposed restructuring of the system, many private insurers and health care providers will continue to do business as independent firms whose interests do not coincide.

There are three major areas in which government action might be considered: 1) providing leadership in the adoption of standards for electronic medical payments and other transactions and exchanges of health information; 2) establishing a system of unique identifiers for people, providers, and payers; and 3) establishing a more consistent regulatory environment for interstate exchanges of health information.

Standards

The federal government has already played a major role in establishing the current level of standardization. For example, in the area of electronic medical payments, HCFA's commitment to electronic claims-filing and its adoption of EDI standards have caused many providers and private payers to use these technologies. Further steps by HCFA—for example, offering truly expedited payment to providers who file electronically (instead of making delayed payment to those who make paper claims, as is currently the case) —could encourage more providers to make the necessary investments needed to comply. HCFA's early adoption of EDI standards for other forms and transactions could also inspire other payers to make use of them. HCFA's ongoing plans to establish a national payer file and to automate secondary payments should also serve as an example of how to simplify the complex process of coordination of benefits. Thus, one option for federal action is to *continue to influence the standardization of health care information transactions through the federal government's role as a major insurer.*

However, even HCFA's leadership will not ensure universal compliance with standards among all payers and providers, and it is likely that widespread compliance is needed in order to realize noticeable savings. As long as some set of participants does not comply, many others will have to maintain separate systems or multiple versions in order to do business with them. The information involved is very complex, and certain classes of participants—payers, state governments, and others—will continue to create the need for new types of data for their own purposes, but not necessarily those of their trading partners or the system as a whole. If they have either money or licensing authority on their side, their trading partners will have to comply with their demands in addition to the standard.

Given that near-universal compliance seems to be important, but is not being achieved as yet, Congress may want government to take a more active role in administrative simplification. Thus, a more active approach would be for Congress to consider *requiring the adoption of industry-developed standards for core electronic transactions, including maximum data sets, and setting timetables for their implementation.*

This option suggests the adoption of standards for a small set of core transactions within the near future. It assumes that the transition from a fee-for-service environment to a managed care environment is going to be a gradual one, and that for a number of years it will be worthwhile to make the basic fee-for-service transactions as efficient as possible. This option is also limited in that its aim is not to mandate sweeping requirements for implementing electronic transactions, but rather to focus on a small set of transactions. Core transactions include: claims and billing, payment and remittance advice, eligibility inquiry, enrollment, and coordination of benefits. Standard forms for managed care transactions, such as the encounter report, could also be considered in this group. These are areas where the voluntary standards process is well advanced. Requiring adoption of standards for other transactions might be considered in the future.

The option includes a requirement for *maximum data sets* for each transaction. It will be necessary to obtain consensus from providers and payers about what information is needed for the transactions, and then ensure that participants may not unilaterally increase information requirements that would lead to the proliferation of nonstandard forms.

A requirement for universal compliance with an electronic transaction system would necessarily create problems for some providers and payers, particularly small ones. Clearly not all providers and payers will be able to handle electronic transactions or modify their proprietary systems to meet standards within any given timeframe; however, they should be able to contract with community health information networks, clearinghouses, electronic medical claims services, or other firms who can provide these services for them.

Unfortunately, a government-imposed standards-setting process would require some central focus of authority to set timetables and to ensure compliance. Therefore, a necessary corollary to the option discussed above would be to *charge a government agency with responsibility and authority to set standards and data definitions for administrative transactions in consultation with industry groups, and to manage changes to standards over time; or create an agency or commission for this purpose.*

Establishing a central authority, whether within an existing agency or in a new commission, is also a cost—one that would be shifted from the health care system as a whole to the government. However, it is unlikely that standards and timetables will be adhered to unless someone is in charge.

Possible disadvantages of requiring standardization and creating an authority—for example, locking into a standard too soon—do not appear to be problems for electronic medical payments at this time, at least for core transactions. Industry groups have made progress with standards for the basic core transactions and preliminary versions are available for many. There is a need, however, to ensure that the standards are implemented in the same way so their use is uniform. Industry input, from both payers and providers, is definitely needed for this. Clearly, if the agency or commission attempted to develop standards de novo, many unnecessary costs could be incurred; therefore it would have to work closely with industry groups already in existence. A number of industry groups have voiced support for greater government involvement, including actions to speed the standards-setting process.

Standard Identifiers for Individuals, Providers, and Payers

Consistent with the above options, another area for nationwide action would be to *establish a system of unique identifiers for patients, providers, and payers.*

Controversy continues about the particular system of identifiers to be used for individuals. In the past, OTA has cautioned against use of the SSN as a national identification number of any kind, largely on privacy grounds. OTA has suggested in earlier work that a new numbering system, with legal protections against misuse built in from the beginning, would be more appropriate. Supporters of the SSN argue, with some merit, that the disadvantages cited for the SSN are bound to afflict any numbering system eventually, even one that is developed from scratch. With modifications, such as a check digit or other additional digits, the SSN may be the fastest and possibly the lowest-cost option for establishing a numbering system.

Identifier systems that meet the needs of both private sector and government users would be most useful. HCFA has made efforts to include a variety of public and private stakeholders in the development of its national provider identifier (NPI). That system, which HCFA proposes to implement for Medicare providers in 1996, has the potential to be expanded into a universal system. Expanding the NPI to include non-Medicare providers would require congressional action to allow HCFA to open up the system and to establish which agency should administer it. Similarly, HCFA's efforts toward developing a payer registry and automating the secondary payment process could serve as the basis for establishing a national, automated coordination-of-benefits system for private payers.

▮ Consistent Regulatory Environment

Some state governments, under the influence of industry associations and other groups, are attempting to change state legislation that limits the development of computer-based patient records. However, the variety of state legislation that affects electronic health information is still bewildering and poses a barrier to the efficient development of interstate electronic commerce in health care. One option is to *encourage the passage of uniform state legislation with regard to privacy and confidentiality, allowable storage media, and standards for health information.* A number of industry groups are already working with legislatures to enact uniform legislation. In addition, the Department of Health and Human Services has recently been tasked by the Administration to take the lead in developing model state privacy laws and model institutional privacy policies for health information. Such leadership by a federal agency may be useful in speeding the adoption of new information laws.

Privacy and confidentiality are particularly important areas in dealing with health information; if there is little confidence that an electronic medical information system will protect them, then providers and patients will be unwilling to use it. If the process of revising legislation on a state-by-state basis is seen as too time-consuming, or not sufficiently effective, then some additional federal intervention may be necessary either to support uniform legislation or to provide federal legislation. In this case, Congress may wish to e*stablish federal legislation and regulation with regard to privacy and confidentiality of medical information, as well as storage media for medical records and electronic data standards for storage and transmission of medical information.* A corollary to this option is to *charge a government agency, or create a committee or commission, to oversee the protection of health care data; to provide ongoing review of privacy issues; to keep abreast of developments in technology, security measures, and information flow; and to advise Congress about privacy matters in the area of health care information.*

The purpose of these options is to create a national environment where electronic commerce and the development of computer-based patient records is not discouraged by local differences in regulation. This would establish a minimum *floor* so that interstate commerce and information exchange can be maintained. There is still a need for considerable research on the computer-based patient record and other kinds of health information. Detailed standards about the computer-based patient record within a particular provider organization cannot be legislated or established by regulation at this time, and, in fact, such regulation may never be desirable. However, minimum standards for the storage and protection of health information, and for its exchange among institutions, may now be in order.

Many violations of security, privacy, or confidentiality are caused by *insiders*—trusted individuals who exceed their authority or put information they are authorized to have to an unauthorized use.[80] Establishing clear and uniform law to protect privacy and confidentiality, along with civil and criminal penalties for violations, would encourage organizations that handle electronic health care information to establish strong internal policies and procedures, which will be as important as technological protections for information. With regard to privacy and confidentiality, an earlier OTA report cited seven provisions to be considered in any federal legislation affecting health information:

1. Define the subject matter of the legislation, *health care information*, to encompass the full range of medical information collected, stored, and transmitted about individuals, not simply the patient record.
2. Define the elements comprising invasion of privacy of health care information and provide criminal and civil sanctions for improper possession, brokering, disclosure, or sale of health care information, with penalties sufficient to deter perpetrators.
3. Establish requirements for informed consent.
4. Establish rules for educating patients about information practices; access to information; amendment, correction, and deletion of information; and creation of databases.
5. Establish protocols for access to information by secondary users, and determine their rights and responsibilities in the information they access.
6. Structure the law to track the information flow, incorporating the ability of computer security systems to monitor and warn of leaks and improper access to information so the law can be applied to the information at the point of abuse, not to one “home” institution.
7. Establish a committee, commission, or panel to oversee privacy in health care information.[81]

These principles will continue to be useful in designing uniform state or federal regulation with regard to health information security, privacy, and confidentiality.

[80] Office of Technology Assessment, op. cit., footnote 69.

[81] Office of Technology Assessment, op. cit., footnote 60, p. 87