AMERICAN HEALTH CONSULTANTS®

HOSPITAL PAYMENT & INFORMATION MANAGEMENT™

INSIDE

DECEMBER 1998

VOL. 16, NO. 12 (pages 177-192)

American Health Consultants® is A Medical Economics Company

New law encourages discussion of Y2K readiness information

Exceptions, other disincentives may limit its effectiveness

Legislators hope that a new law signed by President Clinton on Oct. 19 will encourage communication about year 2000 (Y2K) readiness among manufacturers and organizations. Exceptions in the Year 2000 Information and Readiness Disclosure Act and other disincentives to communicate, though, threaten the bill's effectiveness.

The law, also know as the Good Samaritan Act or the Amnesty Bill, is designed to limit the liability of companies that share the compliance status of their products. The law protects only certain statements of compliance; it does not shield the manufacturer from the liability associated with the actual failure of the product.

"Although the Department of Justice has already indicated that competitors in an industry who merely share information on Y2K solutions would not be in violation of the antitrust laws, this act creates a specific exemption from the antitrust laws for these activities," Clinton said when he signed the bill. The law applies to statements made between July 14, 1998, through July 14, 2001. The law also extends protections to some previously made disclosures if proper notice is given within 45 days after the date of enactment of the law.

"Some hospitals are instituting gag orders on their employees, prohibiting them from talking outside the hospital about their year 2000 projects."

The law also directs the administrator of General Services to create, maintain, and promote a national Y2K Web site to assist customers, small businesses, and local governments in obtaining information about Y2K processing of computers, systems, products, and services.

Not only is the law supposed to encourage manufacturers to talk about their own products, it also encourages hospitals' staff to talk to each other about what they know or think they know about Y2K readiness, says **Joel Ackerman**, executive director of Rx2000 Solutions

Institute in Minneapolis. Rx2000 Solutions Institute is a member-supported organization helping the U.S. health care system prepare for year 2000.

"The whole purpose of this readiness act is to have something where the manufacturers can say, 'Here's what we think we are doing,' and for the users to say, 'That means we need to test this or maybe we don't need to test this so much,'" says **Diane J.P. McKenzie**, a partner in charge of health care technology law at Gordon & Glickson, a Chicago information technology law firm.

"The act is structured in a way that doesn't allow the user to say, 'I'm going to sue you because you were wrong.' That's the intention," McKenzie says. "I have a whole team of litigators, though, who say there are a number of ways that they can probably get around that, in the way it's been enacted through some of the fraud provisions." For example, the court can determine that the maker's use of the year 2000 readiness disclosure amounts to bad faith or fraud, or is otherwise beyond what is reasonable to achieve the purposes of the law. "I'm not sure necessarily that Congress and Clinton have accomplished their goals because the exceptions may engulf the rule," he adds.

Other reasons to keep your mouth shut

Manufacturers are put in a bind with the Y2K issue, McKenzie says. "If they say 'This is what we think right now' and it turns out that the statement is wrong, and there's some probability that whatever they think can be wrong because they are still testing — then they have exposed themselves to legal liability, much greater than if they had kept their mouths shut."

Ackerman also finds that many hospitals are keeping quiet about Y2K compliance issues."When we try to get hospitals to open up and talk about what they are doing to get ready for year 2000, we are finding everyone clamping down on communications," he says. "Some hospitals are instituting gag orders on their employees, prohibiting them from talking outside the hospital about their year 2000 projects."

One reason for using a gag order is the fear of being sued because someone didn't like what you said about a product. "This law will help alleviate that, although I am told that the law contains loopholes, and it's not a total protection," Ackerman says. "There is still some risk, but it is reduced."

The new law, however, addresses only one piece of the problem, Ackerman says. Other problems include:

❒ **Fear of the impact on customers or other clients or partners.**

"If I'm a major East Coast metropolitan medical center, and I find that my intensive care monitoring system will go down and stay down on Jan. 1, 2000, I don't want to talk about that for several reasons," Ackerman says. "I don't want my customers or patients to lose confidence in the hospital because they think we are having all kinds of problems, when in fact we are finding and fixing them." Also, for-profit organizations don't want to lose investor confidence.

❒ **Fear of regulatory interference.**

"If I say that I found a problem with a certain product, it's possible that the regulatory agencies may want to spend time in my hospital understanding the extent of the problem, studying it, and distracting my people at a time when I need to move ahead with fixing year 2000 problems," Ackerman says.

❒ **Fear of losing key resources.**

"If [administrators from] the hospital down the street wake up today and decide to get moving on year 2000 [projects], they will need to find skilled, knowledgeable resources that they can hire quickly," he says. The most visible Y2K problem: Solvers may become targets for headhunters or recruiters.

Because of all these kinds of problems, the new law will probably not open the "information floodgates," Ackerman says. "I'm hoping that it will help to improve the information flow, but my expectations are not that high." ■

COMING IN FUTURE MONTHS

- OIGs 1999 work plan
- The ins and outs of vertical integration
- Speech recognition system slashes transcription costs
- Why CHINs are a dying breed
- AHIMA offers a compliance program

Confidential exchanges in the electronic age

Docs, patients must know how, when to e-mail

Bob Jones needs a referral from his family doctor. Not wanting to wait on a telephone call, he e-mails the request. The next day, he has a reply with the referral.

John Smith sends a message to his doctor complaining of chest pains. The physician is not able to read his e-mail for several days and is alarmed when he gets the message.

The above scenarios show the importance of establishing a policy about how and when to use e-mail communication between physicians and patients.

Whether to allow e-mail communication at all is no longer the question for health information professionals. More and more computer-savvy patients prefer e-mail for nonemergent requests because they can ask their doctors questions directly without having to wait by the telephone for a reply.

Trend for e-mailing will increase

This trend will only increase, says **David Sanders**, MD, CEO and founder of Salu.net, a provider of Internet-based private networks for physician practices and health professionals in Portland, OR.

"Communication will migrate aggressively within the next five years to e-mail-based communication," he predicts. "[E-mail] will change the way doctors, staff, and patients communicate."

A medical practice is 90% communication, he explains. About half of that communication is face-to-face. The other half is communication by other means such as phone or fax. "The problem with the phone is that it requires the doctor and the patient to be available at the same time," Sanders says. "It's hard to do that when doctors are under such high time pressure. E-mail separates out the requirements for two folks being in the same place at the same time."

"There is an increasing encroachment of electronic [communication] in the physician-patient relationship," adds **Faith McLellan**, PhD, faculty associate in the department of anesthesiology at the University of Texas Medical Branch at Galveston.

McLellan learned about e-mail communication while researching her dissertation about patients' illness experiences. Even though she found that physician-patient e-mail communication is becoming more common, many physicians are still uncomfortable using it.

"In a larger conceptual universe, it upsets the balance of power," she says. "Suddenly there is information and information management tools in the hands of people who have usually been the recipients of physicians' power and knowledge."

A lot of physicians are computer naive, too, she adds. "They haven't thought about some of the issues such as privacy and confidentiality, and how easy it is to disseminate information to other people through e-mail and how instantaneous it can be."

Watch out what you say

Many patients use e-mail so much that they see it as a natural way to communicate with their physicians, McLellan says. A recent article in the *Annals of Internal Medicine* found that patients see e-mail as creating continuous access to the health care system, something they feel lacking as physicians spend more time on administrative tasks and less time on personal interaction.[1]

E-mail works well when the patient requests general information or sends routine information about a chronic illness. A diabetic patient, for example, might send her physician information about her blood glucose levels. The physician doesn't need to respond right away unless the results are abnormal. "E-mail is the perfect medium for that," McLellan says.

E-mail also provides a way for physicians to filter medical information. Some managed care plans, for example, have a site where they recommend electronic resources on medical information.

In addition, e-mail can allow patients with similar conditions to meet in electronic discussion groups. These groups can be a great relief to both the patient and the physician, McLellan says. "The patients are hooking into a source of support that they don't necessarily get from their personal physicians. It not only provides access — a route of communication between the patient and the physician — but it hooks other people up whose time is better served in discussion, answering questions, and support."

E-mail can be a barrier to patient care, however. Some questions to be considered include: What happens with e-mail communication

Encryption available through Medical E-mail

Providers who are trying to navigate the e-mail territory but don't want to do it themselves might find help through a company called Salu.net. The company offers physician-customized Web sites; secure, encrypted messaging through its Medical E-mail; and permanent message archiving.

"Everything you do in a practice is a legal document," says **David Sanders**, MD, CEO and founder of Salu.net.

"It is important you have a record means to track all of those [e-mail] communications. On a real-time basis, we extract all of the data points that go on, and we archive them in a compressed fashion. If a member wants to go back and retrieve documentation, it's there for them."

The messages are archived for 10 years. "Then we contact members and ask them if they want to receive data backups of their systems. At that point, we will begin to discard records."

The Web sites are used for patient education, practice promotion, and customer support. Patients can retrieve different educational materials, which the physicians have chosen to offer. Patients can also find out more about the practice and even get directions and office hours.

Physicians can access Salu.Net from any system that has Internet capabilities. Salu.net is also integrated, so physicians can access everything in the system by signing on and giving a password.

Salu.net has a training program for users, which urges them to talk to patients about using e-mail. "For example, make it clear to patients that if they are going to use e-mail with you, here is what is considered appropriate content and timeliness," Sanders says.

A newer version of the system will provide a guidance site for patients that tells them how to become an effective user of e-mail with their physicians.

Offering e-mail resources makes physicians seem more current with the times, Sanders says. "Doctors who are on-line are put back in the game. They are more in the partnering mode than an 'outsider' who is not providing information."

Editor's note: For more information about Salu.net, call (888) 288-SALU.

Reference

1. Mandl KD, Kohane IS, Brandt AM. Electronic Patient-Physician Communication: Problems and Promise, *Annals of Internal Medicine* 1998; 129:495-500. ■

between patients and their doctors when the doctor is on vacation or not in the office or not on call? What happens if the server goes down? When will the message be received? What kind of messages are appropriate for patients to send?

"Establishing a policy on using e-mail is a good idea," says **Victor S. Sierpina**, MD, an assistant professor of family medicine at the University of Texas Medical Branch in Galveston. For example, patients should be discouraged from sending emergency or urgent kind of inquiries. They should be aware that their messages might not be answered right away.

Physicians should have a separate office e-mail account than their personal one. They should not use e-mail to communicate abnormal test results or to give bad news.

"You don't want to be discussing psychiatric history or HIV status — something that could be used to discriminate against the patient," McLellan says.

Physician e-mail users also should ensure that electronic communications do not widen the disparity between the haves and the have-nots. Patients without access to computers should receive the same health information, she explains. "You don't want to create a society where the patients who have e-mail are getting better care than the patients without."

Sierpina has one rule of thumb on the use of e-mail: "Don't put anything in e-mail that you wouldn't want to see on the front page of a daily newspaper."

In his experience communicating with patients, he has found that they usually write short messages and generally don't abuse the system, he says. They don't always think about the lag time between the sending and receiving of messages,

however. One of his patients, the man with the chest pains mentioned earlier, luckily had a condition that did not require emergent care.

Another physician is finding that increasingly he is attaching medical information to e-mail messages to educate his patients. ■

AHIMA revises its certification requirements

ART requirement, RRA proviso approved

Future candidates for Accredited Record Technician (ART) and Registered Record Administrator (RRA) certification take note: Revisions to the Standards for Initial Certification were approved by delegates at the 70th annual meeting of the Chicago-based American Health Information Management Association (AHIMA) in October. Both revisions are parts of AHIMA's Vision 2006, an eight-point strategic initiative to move the health information management profession into the next century.

Associate's degree required

One significant change is that after Sept. 30, 2002, candidates for initial certification as an ART will be required to have an associate's degree earned from an accredited health information technology program. ART certification candidates who have completed AHIMA's independent study program will be required to have earned an associate's degree or higher from an accredited college or university. This change will not affect anyone who is currently credentialed as an ART or who obtains his or her credential prior to Sept. 30, 2002.

"The philosophy [in adding that requirement] was that current marketplace trends in all fields demand more education as a prerequisite for being a professional," explains **Belinda Brunner**, AHIMA's director of certification. "Increasing the minimum standard is consistent with that trend."

The new requirement primarily affects individuals completing the AHIMA Independent Study Program in Health Information Technology. Previously, candidates had to have at least 30 semester hours of college level courses. The 2002 date was selected to give individuals in the program due notice of the new requirement.

Many of the certification candidates already have an associate or more advanced degree, Brunner says. AHIMA statistics show that more than 90% of the individuals who sit for the ART certification each year hold at least an associate's degree. The change in standards, therefore, would affect less than 10% of the ART candidates.

RRA proviso added

The delegates also approved a proviso to the Standards for Initial Certification regarding the RRA exam. ARTs who meet certain requirements will be eligible to take the RRA exam between 1999 and 2004.

These requirements mandate that ARTs:

- have at least a baccalaureate degree;
- have received an ART credential on or before Dec. 31, 1999;
- have complied with the Standards for Maintenance of ART certification, which means candidates for the RRA exam must be up-to-date on their continuing education hours.

"Prior to the passing of the proviso to the standards for initial RRA certification, ARTs were not eligible to write the RRA exam unless they went through an accredited baccalaureate degree health information administration program," Brunner says.

The limited number of four-year programs, however, have resulted in many practicing ARTs earning baccalaureate and post-baccalaureate degrees in related disciplines.

The proviso's "window of opportunity" has been created to recognize ART-credentialed professionals who have obtained their baccalaureate degree or post-baccalaureate degree in related disciplines and wish to obtain their RRA certification.

The time frame for the proviso is limited because AHIMA is currently implementing a newly approved model curriculum in the fall of 1998 for all of its educational programs, Brunner says. "The new model curriculum intensifies and clearly distinguishes between the differences in the breadth and the depth of health information educational preparation among the [HIT and HIA] levels."

If track programs are approved at the baccalaureate level, AHIMA hopes that four-year degrees will become more accessible. ■

HCFA turns to commercial software to verify claims

Provider compliance tool available

The Health Care Financing Administration (HFCA) in Baltimore has announced that an off-the-shelf software product is being used by Medicare contractors nationwide to check claims for improper coding.

HCFA awarded HBOC, a health care information systems vendor in Atlanta, a $20 million, two-year contract to allow Medicare contractors to install more than 200 computer "edits" from a portion of HBOC's ClaimCheck automated clinical editing database onto their own claims processing systems. (Edits are computerized instructions that verify claims information.) In addition, HCFA says it may implement additional edits during the next two years.

"I am determined to use off-the-shelf products whenever possible and as quickly as feasible," says HCFA Administrator **Nancy-Ann DeParle** in a statement.

Providers can access the ClaimCheck database through HBOC's Medicare medical necessity and prebilling compliance tool for providers, Pathways Compliance Advisor. According to an HBOC spokesperson, this tool is a slightly rewritten version of the database but still checks for the same information.

HFCA tested ClaimCheck's edits during a pilot project in Iowa in 1996, which tried to improve the accuracy, consistency, and efficiency of Medicare claims processed through HCFA intermediaries and local carriers. HCFA determined the edits should be used by other Medicare contractors

Systems like ClaimCheck "make sense of the complex coding arena and offer good news for both payers and providers," says **Jay Gilbertson**, HBOC president, chief financial officer and co-chief operating officer. "By taking the guesswork out of coding, payers have the potential for large-dollar savings, and payer feedback helps providers make accurate coding choices on future claims."

The new edits are in addition to the more than 100,000 edits developed for HCFA under the system known as the Correct Coding Initiative, first implemented in 1996.

HCFA says the initiative is part of Medicare's ongoing activities to detect and prevent inappropriate payments. Earlier this year, a General Accounting Office report had also urged HCFA to buy or lease existing comprehensive commercial claims auditing edits and begin a phased national implementation.[1]

Reference

1. *Medicare HMO Institutional Payments: Improved HCFA Oversight, More Recent Cost Data Could Reduce Overpayments.* HEHS-98-153. ■

Q & A Corner

Pre-plan replacement of outdated computers

By **Garry McGonigal**
President
Corporate Environment Consultants
Tecumseh, Ontario, Canada

When Garry McGonigal wears his chief information officer "hat" for a large information systems operation, he often has to dispose of and replace outdated computer equipment. Here is what he recommends to information officers undergoing the same process.

Q: What issues should you consider when it comes time to replace your computer equipment?

A: Disposal and replacement of old with new computer equipment can be a complex, time-consuming process. If there is sufficient scale, then all of the process could be contracted out or included in an evergreen leasing and maintenance process, whereby your current inventory is bought out and replaced with brand new equipment, and then replenished with up-to-date equipment as predetermined by the lease / maintenance schedule. Whichever methods are selected, it has to be a planned and schedule endeavor. Network capacity could be put at serious risk just due to volume.

(Continued on page 187)

(Continued from page 182)

Also, replacing older legacy devices, such as dumb terminals, with new personal computers (PCs), may drop a substantial load on an older, UNIX-based system, for example. Such systems were accustomed to character-by-character activities and slow printer response. Bringing on new equipment, probably on a much higher-performance network but still using the older server applications, could actually overload the servers.

In addition, going from a setup where the end user had standalone word processing and spreadsheet applications to a server-based office automation setup could actually put the end user applications at risk. For example, if the server went down, many users would go down with it. Whereas before, if one user's PC went down, chances are that only that user was affected. On a positive note, central backup of most of these users' data can now take place.

Also, don't forget that typically when you replace an individual's "piece of junk" with the latest and greatest, the move will most certainly upset the status symbol balance in any office environment. It is equally important not to allow the senior executive to use this allocation of new equipment as his or her way to give personal favors. The process will then become very illogical and will set all sorts of precedents throughout the organization, many of which will keep compounding themselves over and over: Folks will somehow get to their executive who will then try to persuade the senior people in information services (IS) to bump someone else (from getting the new equipment), again and again.

All of the equipment replacement process has to be carefully planned out, scheduled, and the political elements addressed ahead of time. Eliminating surprises is the key. The most important axiom to remember is never to promise more than can be delivered — it is best not to disappoint.

Q: Should you look into getting replacement parts first?

A: Getting replacements parts for older PCs and peripherals is very difficult. The parts are also expensive, compared to what an up-to-date Pentium-based piece of equipment would cost. Generally, hard disks, mother boards, monitors, and graphic cards fail due to age and / or electrical power surges.

In addition to the parts cost is the cost of having someone on staff do the repairs, assuming that it is too expensive to farm it out, and / or there are very few people available to do the work. This also means that your precious IS staff have to keep the old software drivers around for this equipment and older versions of such software as Microsoft Office, and they have to remember even how to work with Windows 3.11, for example, and its family.

It is tough enough on this staff just trying to keep the Pentiums going, let alone some of that older equipment. More frightening is that there are databases that will only run on this older equipment, with no upward migration path. When that equipment fails, the application is also gone — sometimes a very daunting future.

Q: Should you toss the equipment or try to give it to someone else in your organization?

A: Depending on the age of the equipment, you might not find anyone interested in taking it off your hands for free. I have been down that path too often. I have tried school boards, teen action groups, technical college repair shops, etc. Many don't even want 486's.

You can give some of the older software, fully licensed, away to schools. Corel, Microsoft, or Lotus generally has an entire program, documentation, and forms to allow for such license transfers.

Another method of disposing of older equipment, and probably the first one to try, is to have an employee sale or giveaway. Pick a Saturday, advertise in advance, and establish the policy on how the equipment will be given away — as is, first-come, first-served. Provide a receipt to those taking the equipment that states the serial numbers and transfer of ownership. Since this equipment is a depreciable capital asset, accounting needs to be involved in this process.

Generally, before we tried either to give anything away or throw the equipment into a garbage bin, we had to remove the hard disks, low-level format them, and then run a substantial magnet over them to ensure that the data can never be recovered. This process generally destroys the hard disk.

Cascading not-so-bad computer PCs to elsewhere in the organization is a real nightmare for IS. To replace someone's old system with a brand new one means all of the existing data has to be transferred to the new equipment. The old PC has to be taken back to IS, totally backed up, and held in stock for at least two weeks because more

data may have to be retrieved from the original. Then the old PC has to be thoroughly checked, possibly refurbished, given to the next person, and the cycle keeps repeating itself. It never seems to fail that the second-hand computer, once moved, has a shortened life expectancy; it soon experiences a hardware failure. All of this is very time-consuming for IS, and each cascade could easily take five hours if there are no problems (in a large organization).

The bottom line is to keep the old junk for parts until the entire inventory of that equipment is out of the corporation. Contact a business equipment company (usually the larger ones with branches throughout the country and/or a region) and see if it will take the equipment off your hands at no charge. Or, if you go to a lease/maintenance plan, see if they will take it all.

Q: How do you handle the transfer of information from the old PC to the new one?

A: If data have to come over to the new PC, and usually the old one is not on a network, then the transfer is either via a portable zip disc with parallel port connection, or laplink to a laptop. If a writeable CD unit is on the system, then the transferred data will get burnt into a CD and verified. When the new machine is ready, the CD is loaded and the data is transferred. To start it all off, it is essential that a document and checklist form be provided to the end users to put the responsibility on them to formally identify what they want transferred. This list is then used by IS to check off everything that comes across. The CD is provided to the end users as their own record of the old data and as a backup of that data.

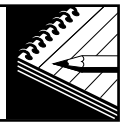
We have used a computerized inventory system to inventory all equipment and software. When preparing for a transfer, we have added to this inventory the location of end-user files, databases, etc.

Hopefully, the end users did not complicate their PCs too much, thus making it rather difficult for IS to find the data. Dedicating specific staff to this process goes miles in ensuring consistent and quality work.

Q: What about the transfer of confidential information?

A: Depending on the level of security clearance required, sometimes extracting and storing the data all has to remain in the physical presence of the end user. If a "go-between" device is used, such as a laptop, then not only does the data have to be "scrubbed" from the laptop, it also has to be certified as complete by a security officer who is familiar with these processes and/or audit control. If a zip drive is used, similar processes must be followed. If the data is to burnt into a CD, then the host PC has to be tightly controlled and again security measures involved, or the host PC and burning CD must be brought to the end-user location. ■

GUEST COLUMN



Rapid industry change demands best-of-breed

By **Kent J. Sacia**
Consulting Actuary
Milliman & Robertson
Seattle

Provider reimbursement continues to shift from a fee-for-service structure to a risk-based structure. Providers now commonly accept primary care, specialty, and global capitation in addition to per-diem and case-rate reimbursements.

The future likely holds outcome- and performance-based reimbursement formulas for many health care providers. These risk-based reimbursement systems necessarily change provider business management needs, causing providers to perform new administrative activities.

Although the type of risk taken determines what new capabilities are needed, most providers assuming risk need to do the following to be successful:

✔ track operational performance measurements;
✔ administer capitation and other alternative forms of payment while continuing to administer fee-for-service payments;
✔ administer incentive/risk pools;
✔ administer stop loss.

To successfully manage this new risk, providers must gain more control over the management, approval, and payment for health care services. Because these functions are traditionally under the purview of the health plan, most provider

organizations are not prepared to assume these responsibilities.

Furthermore, because these functions rely heavily on advanced information systems, provider organizations must make an investment in their future by locating and implementing appropriate technology. When developing an effective system strategy for the new requirements of the health care industry, it is first important to understand that there are no silver bullet vendor solutions.

Health care delivery and risk models are evolving so quickly that individual software developers are unable to keep up. Typically, it takes a vendor two years to fully develop a large-scale application. Assuming the vendor fully understood the leading-edge requirements of the industry as it undertook the development, it probably did not predict the evolution of the requirements during those two years.

Successful software vendors, therefore, are typically niche players that support only a limited range of functionality. Successful provider companies employ a best-of-breed model in their system strategy. This model targets the purchase and implementation of the best products for each distinct functional requirement.

For example, a mid-sized integrated delivery system with a mature risk model may maintain best-of-breed systems for:

- ✔ practice management;
- ✔ medical management;
- ✔ claims processing and capitation;
- ✔ credentialing;
- ✔ data analysis and reporting.

Because rapid industry change requires leading-edge business and technology knowledge, most provider organizations are not well-equipped to build their own core system applications. The provider should, therefore, buy core system elements from best-of-breed vendors whenever feasible.

The provider may then build surrounding applications where its unique needs are not fully met by software vendors and to complete required interactivity. A typical application that is built internally is risk pool management. Many organizations develop unique methods of sharing risk. These organizations often build interfaces from utilization and membership systems into an internally built risk-tracking and allocation system.

The ultimate value associated with purchasing best-of-breed systems is realized over the life of the organization. As the industry business models change, these best-of-breed niche vendors are better able to enhance their products to meet the changing requirements.

A prime example of this ability is shown in vendors that offer medical management software distinctly from claims administration systems. These vendors have quickly added remote case management capabilities and have successfully integrated clinical guidelines and pathways.

Once an organization employs the best-of-breed systems model, a key issue becomes the integration of data across these various systems. Vendor systems do not typically integrate easily with other systems. The most common interface mechanism is through batch data extraction and loading.

Data warehousing technology has emerged as the most effective system and data integration tool. The data warehouse captures and stores critical information from multiple system sources.

Data warehouses also serve as the hub for information moving from one system to another or from one organization to another. Additionally, the presence of the data warehouse allows the organization to more quickly add and integrate new systems and functionality. ■

Health information organizations laud bill

Legislation protects privacy of patient information

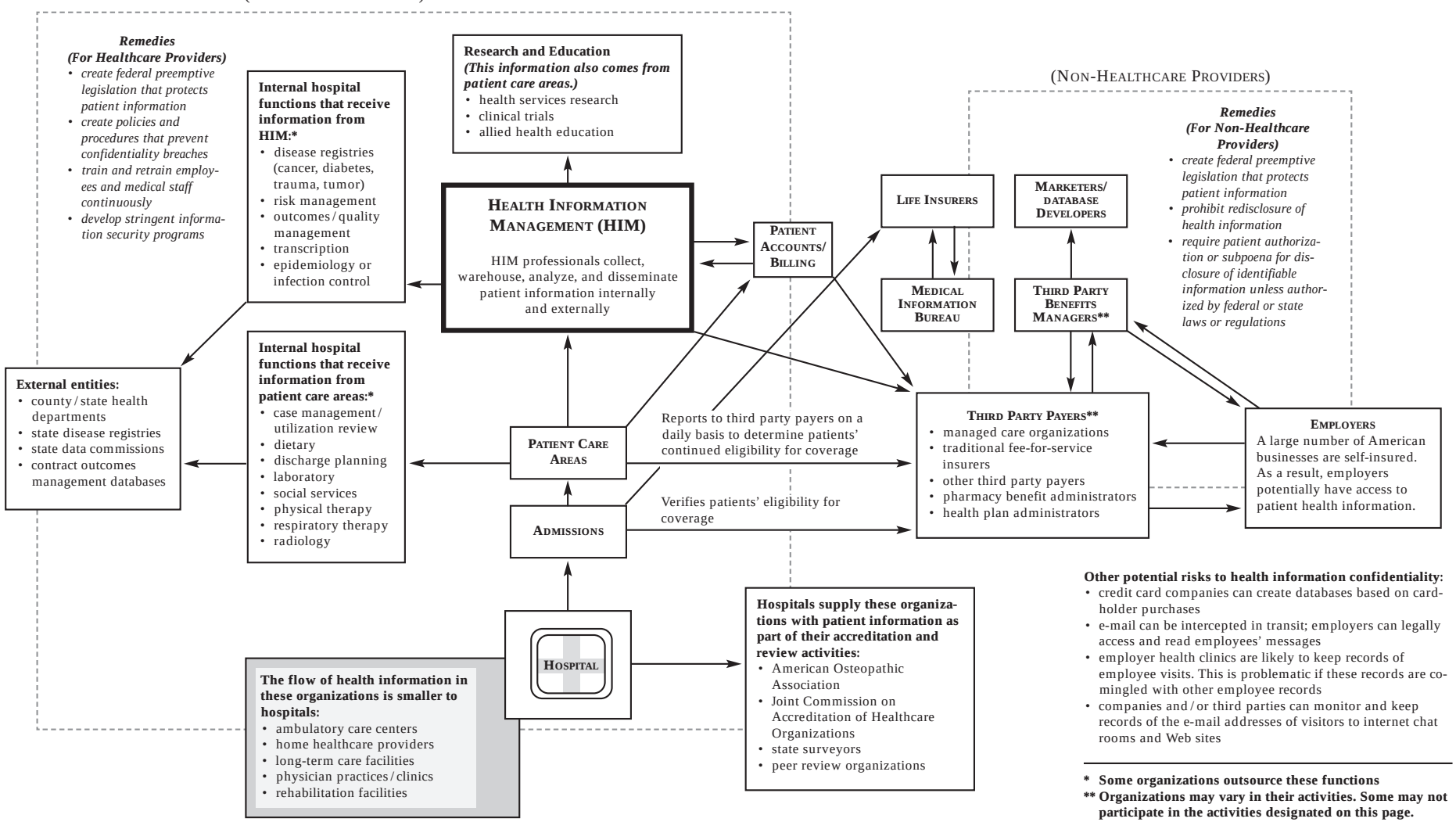
For the first time, legislation introduced in the U.S. Senate would establish the confidentiality of individually identifiable health information. The "Medical Information Protection Act of 1998" was introduced Oct. 9 by Sen. Robert F. Bennett (R-UT) and cosponsored by Sen. Connie Mack (R-FL).

"The bill strikes a hard to achieve balance between protecting the confidentiality of a patient's health information while not impeding the provision of patient care or the operations of the nation's health care delivery system," says **Kathleen A. Frawley**, JD, MS, RRA, vice president for legislative and public policy services at American Health Information Management Association (AHIMA) in Chicago.

Congress must pass legislation governing

(Continued on page 191)

Flow of Patient Health Information Inside and Outside the Healthcare Industry



Source: American Health Information Management Association, Chicago.

electronic health information before August 1999, in accordance with the Health Insurance Portability and Accountability Act of 1996. If Congress does not act by that time, the responsibility for the regulation passes to the secretary of Health and Human Services in Washington, DC.

Bennett mentioned the support of several organizations in his address to the Senate. In addition to AHIMA, he mentioned the American Hospital Association (AHA) in Washington, DC.

Confidentiality is a critical concern

"Comprehensive confidentiality legislation is critical to thousands of patient who come through the doors of our nation's hospitals each day," says AHA president **Dick Davidson**. "We commend Sen. Bennett for his leadership and guidance on an issue that is relevant to everyone."

Here are some of the provisions of the bill:

- It gives patients in all states access to their medical records.
- It establishes full federal preemption of all state confidentiality laws, with the exception of some public health laws. It also sets a uniform standard to eliminate the current variety of state statutes and regulations.
- It recognizes the need for confidential medical information to move appropriately and in a timely manner within groups and systems of providers without impeding the quality of care.
- It broadly applies not only to providers, payers, and employers, but also to law enforcement agencies. The bill sets a national standard for how law enforcement officials can gain access to confidential patient records.
- It contains criminal and civil sanctions to provide remedies against wrongful disclosure of health information.

AHIMA has worked closely with Sen. Bennett for several years on confidentiality issues, says **Jack Segal**, AHIMA's director of public relations. To stress the importance of the need for confidentiality legislation, AHIMA released a flowchart that shows the large number of individuals and organizations that have access to a patient's medical information. **(See chart, p. 190.)**

"One of the things we wanted to do [with the flowchart] was to educate the public, the media, and members of Congress about who has access to medical records and the extent that they have access to them," Segal says. "We thought the chart would be helpful in terms of moving the discussion forward." ■

NEWS BRIEFS

Senator releases names of noncompliant vendors

Medical device vendors that did not respond to the federal Food and Drug Administration's (FDA) request for a statement of their devices' year 2000 compliance status can now see their names printed in the Sept. 23 *Congressional Record*.[1]

Hospital Payment & Information Management (ISSN# 1074-8334), including **DRG Coding Advisor**fi, is published monthly by American Health Consultantsfi, 3525 Piedmont Road, N.E., Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodical postage paid at Atlanta, GA 30304. POSTMASTER: Send address changes to **Hospital Payment & Information Management**, P.O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291, Hours of operation: 8:30-6:00 M-Th, 8:30-4:30 F, EST.

Subscription rates: U.S.A., one year (12 issues), $499. Outside U.S., add $30 per year, total prepaid in U.S. funds. One to nine additional copies, $250 per year; 10 or more additional copies, $150 per year. Call for more details. Missing issues will be fulfilled by customer service free of charge when contacted within 1 month of the missing issue date. **Back issues**, when available, are $44 each. (GST registration number R128870672.)

Editor: **Sue Powell Coons**, (614) 848-5254 (suby33@aol.com).
Publisher: **Brenda Mooney**, (404) 262-5403, (brenda.mooney@medec.com).
Managing Editor: **Kevin New**, (404) 262-5467, (kevin.new@medec.com).
Production Editor: **Ann Duncan**, (404) 262-5463.

Editorial Questions

For questions or comments, call **Kevin New** at (404) 262-5467.

Angered that less than 40% of the vendors responded to the survey, Sen. **Christopher Dodd**, (D-CT), and co-chair of the Senate's Year 2000 committee, requested that the names of the non-respondents be published "for all Americans to see."

Of the nearly 1,935 medical manufacturers surveyed by the FDA in June, only about 755 replied, according to Dodd. He told his fellow senators that he had been shocked to learn of the "unacceptable low level" of compliance.

"I made it clear [at the July 23 committee hearing] that this sort of attitude was stunningly short-sighted and could only cause harm to both the maker and the users of these devices," he said.

"It is my hope that [publishing the names of the vendors] will serve as a wake-up call to other industries to be vigilant, responsible and proactive in their efforts to ensure that Americans wake up to a wonderful new year on January first of the year 2000," Dodd said.

Reference

1. 105 *Congressional Record* S10790 (Sept. 23, 1998). ▼

House panel gives government a 'D' for 2000

A House panel gave a "D" grade in early September to the federal government's overall efforts to fix the year 2000 computer problem, according to the Associated Press.

The panel predicted more than one-third of the most important computer systems won't be fixed in time, and it estimated the government will spend $6.3 billion on the problem. That is higher than a $5.4 billion estimate the Office of Management and Budget (OMB) in Washington, DC, previously projected.

OMB didn't count estimates from some agencies because it was still trying to determine whether those figures were "appropriate," says OMB spokeswoman **Linda Ricci**. That amount includes $550 million for the Health and Human Services Department and $295 million for the Treasury Department.

Five agencies criticized in the past for their lack of progress, including Health and Human Services, each earned individual "F" grades, although the Defense and Transportation departments improved slightly since June to a D. The Justice Department fell to an F.

"This is not a grade you take home to your parents, and it is definitely not a grade to take back to the voters and taxpayers," says Rep. **Stephen Horn**, (R- CA), who is chairman of the technology subcommittee for the House Government Reform and Oversight Committee.

Others receive failing grades

Other agencies earning an F from Horn's subcommittee included the Energy, State, and Education departments, along with the Agency for International Development.

Three agencies earned an A: the Social Security Administration, the National Science Foundation, and the Small Business Administration.

The subcommittee, which periodically issues its Y2K report cards, says that its $6.3 billion estimate was based on figures submitted by 24 departments and agencies, which they also submitted to the OMB.

Horn also criticized some agencies' plans to fix the problem by replacing affected computers, saying that could lead to further delays. "When was the last time you heard the government putting a new computer in place on schedule?" asked Horn. "There is no room for the usual slippage. There is no margin for error." ■