AMERICAN HEALTH CONSULTANTS®

HOSPITAL PAYMENT & INFORMATION MANAGEMENT™

INSIDE

FEBRUARY 1999

VOL. 17, NO. 2 (pages 17-32)

American Health Consultants® is A Medical Economics Company

Clinton announces Medicare package to fight fraud, save tax dollars

Will the legislation just add another layer of regulators?

President Clinton announced in December a legislative package that he says will save Medicare $2 billion over the next five years by fighting fraud, waste, and abuse. The president also announced administrative efforts to ensure that Medicare contractors are cracking down on fraudulent activities.

"The current federal administration has certainly shown that it is serious about rooting out fraud and abuse so that the Medicare dollars can be well-spent on appropriate and much-needed health care," says **Sue Prophet**, RRA, CCS, director of classification and coding for the American Health Information Management Association in Chicago. "I'm not surprised that it is putting more efforts in place to do this."

Provider organizations, however, have been concerned that government fraud efforts might not make the distinction between billing errors and outright fraud. The president's announcement renewed those concerns and added a few others, as well.

Pieces of the package

The president's legislative package is part of his fiscal year 2000 budget. The president's proposals include:

❒ **Eliminating excessive Medicare reimbursement for drugs.**

The administration's proposal bases Medicare payments on the actual acquisition cost of these drugs to the provider, eliminating markups and substantially reducing Medicare costs. "Under current law, Medicare loses hundreds of millions of dollars each year by paying as much as 10 times more than the private sector does for certain drugs," Clinton said in his announcement. "It's just wrong."

"I continue to find it offensive that the President lumps reimbursement issues with fraud and abuse, says **Mary Grealy**, JD, senior Washington counsel for the American Hospital Association's (AHA) office in Washington, DC. "They don't belong together."

❒ **Eliminating overpayments for Epogen.**

A report from the Office of Inspector General (OIG) found that the current reimbursement rate exceeds the current cost of the drug by at least 10%. This proposal reduces Medicare reimbursement to reflect current market prices.

❒ **Preventing abuse of Medicare's partial hospitalization benefit.**

This proposal ensures that Medicare only reimburses for services actually given by placing stricter controls on the provision of services.

"We know [OIG] found some problems," Grealy says. "As always, we want to make sure they don't go overboard and restrict access to what are necessary services. The services should be provided appropriately. That was an important benefit that served a critical need, and I hope they don't wind up extinguishing it."

❒ **Ensuring Medicare does not pay for claims owed by private insurers.**

This proposal requires private insurers to report all Medicare beneficiaries they insure to the Health Care Financing Administration (HCFA) in Baltimore and gives HCFA greater authority to fine these insurers.

❒ **Empowering Medicare to purchase cost-effective, high-quality health care.**

Currently, Medicare has limited authority to contract out with institutions that have a track record of providing high-quality care at a reasonable price. This proposal expands this authority to urban areas that have multiple providers.

❒ **Requesting new authority to enhance contractor performance.**

This proposal would give HCFA authority to contract with a wider range of carriers and terminate providers they see necessary. HCFA also would have greater authority to oversee contractor performance.

The president's announcements about administrative efforts to crack down on fraud and abuse include:

❒ **Contracting with special fraud surveillance units to ensure detection of fraudulent activities.**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gave new authority to contract with specialized fraud surveillance units or "fraud fighters." The first fraud unit will begin investigating suspected offenders this spring.

"Our concern is that there seems to be a piling on, in a layer upon layer, of entities that will be auditing providers," Grealy says. "We're beginning to worry that people are going to be asking for provider records left and right."

Coordinating the fraud fight

The AHA is also concerned that the fraud-fighting effort isn't as coordinated as well as it could be. "It needs to be done in a targeted way as opposed to casting this wide net."

❒ **Implementing the competitive bidding demonstration for durable medical equipment.**

HCFA will begin a demonstration this spring that will use competitive bidding to decrease payments for hospital beds and other medical equipment.

❒ **Requiring contractors to report fraud complaints to the OIG immediately.**

Contractors often defer reporting cases of suspected fraud to the OIG when the dollar amounts are low. HCFA was to send memorandums to all contractors in December requiring them to refer cases of suspected fraud to the OIG immediately, regardless of the amount of money involved.

"The private sector health care contractors that are responsible for fighting waste, fraud, and abuse too often are not living up to their responsibilities," Clinton said in his announcement. "We recently learned [through an OIG report] that one-fourth of those contractors have never reported a single case of fraud, even though the Inspector General is quite certain that fraud is pervasive in this area."

"HCFA has over-responded to the report by saying that anything you find anywhere, any time must be reported immediately to the OIG.

If you look at the OIG's guidelines, I think they pretty clearly establish that there should be a minimum threshold, that it should be something material," counters Grealy.

Indicators of fraud, such as billing for services that have not been provided, should be referred to the OIG, she says. Otherwise, the fiscal intermediary should be responsible for recouping any overpayment.

"If they are talking about someone making an overpayment and now everything has to go to the OIG, I think that's an inefficient way of doing business and it's casting everyone as a fraudster when that should not be their intent. I don't think it's the Inspector General's view, either," Grealy explains.

"If there is a pattern or some indication of fraud or abuse of activity, we would fully support any efforts to get rid of that," Prophet says. "But there always is the concern that inadvertent errors could be pulled into this process, as well. We don't think people should be prosecuted for errors because there are going to be errors in any industry."

❒ **Announcing a new comprehensive plan to fight fraud and abuse.**

By early next year, HCFA will release a new Comprehensive Plan for Program Integrity to improve efforts to cut down on fraud and abuse. This plan will outline new strategies to fight fraud, including the enhanced use of audits and improved management tools.

Efforts aren't always productive

Although media attention to fraud in the health care industry gives the impression that it is widespread, fraud investigators often don't find that kind of abuse. In an outpatient and lab bundling investigation in Texas, where 400 demand letters were mailed to providers last year, all of the U.S. Attorneys decided to halt their investigation, Grealy says.

Hospitals that had settled with the government and had signed a Corporate Compliance Agreement had their money refunded and the agreement terminated. The financial details were turned over to the fiscal intermediary for whatever review or action, if any, it deemed appropriate.

"That's where it should have been to begin with," Grealy says.

These investigations give the public the impression that most hospitals and physicians are trying to bilk the Medicare Trust fund, Prophet says.

"I don't think that's the case, and I don't think that's what the federal administration is saying. It's important to recognize that the vast majority of health care providers are completely honest, are doing the right thing, and are not committing fraud," she explains.

'We are only talking about a small number of people or organizations. But it's also important to recognize that those organizations could fraudulently bill for a significant amount of money," Prophet adds. ■

Clock reaches midnight hour for Y2K compliance

If at first they don't respond, try, try again

Most hospital information professionals have at least tried to contact their vendors about their systems' year 2000 (Y2K) compliance. That doesn't mean the vendors have responded.

A coordinator for Y2K compliance preparedness processes for health care organizations devised a sample vendor letter and questionnaire that she recommends HIM staff use in both their professional and personal lives.

Laurene West, RN, executive director of Martens-West Year 2000 Consulting in Salt Lake City, sent the letter and questionnaire to her vendors and says the minimum response she has received is a statement about the vendor's Y2K position. **(See sample letter, p. 20, and questionnaire, p. 21.)** The letter and questionnaire should be addressed to the president and chief executive officer of each organization.

"Send letters via registered, return-receipt-requested mail and staple the receipts to your copy of the letter," she says. These records could help provide documentation for any future Y2K legal claim.

Editor's note: This advice is given only as a suggestion based on current information. These documents are not intended to replace advice from your legal counsel, financial advisor, or accountant. Responsibility to prepare for any possible date-related errors or disruptions as a result of the year 2000 is your own.

Laurene West may be contacted through her e-mail address: llw@integrityonline3.com. ■

Sample Vendor Letter

Your name
Organization
Address

Date

President or CEO
Company
Address

Dear_____:

As a concerned consumer of goods and services from your company, I am requesting documentation on your year 2000 certification. The year 2000 virus may affect all products, services, and interactions that depend on date-based calculations for proper operation.

For purposes of this letter, year 2000 certification means that all information systems, applications, macros, spreadsheets, templates, network componentry, microprocessors, plant operation/facility systems, environmental control systems, biomedical devices (including implanted devices), electronic commerce, databases, archives, and related system componentry accurately process date and time data before and after Jan. 1, 2000, and appropriately reflect the year 2000 as a leap year while providing uninterrupted and continued service.

Please respond to the attached questionnaire no later than _____. I am also requesting a statement reflecting the current balance of my account as well as instructions for testing devices with embedded microprocessors, if appropriate, from your organization.

I am encouraging cooperative, community efforts to prepare for the year 2000. Alarm and action now will help to prevent operational disruptions, financial losses, business failures, liability exposure, and civil unrest.

Respectfully,

Your name & organization

Source: Martens-West Year 2000 Consulting, Salt Lake City.

Year 2000 Vendor Questionnaire

1. When did your company initiate the process of fixing year 2000 (Y2K) issues? _____
2. Have you assigned overall responsibility for Y2K efforts to a senior office of your company?
   yes ☐ no ☐
   If so, please provide: name, title:
   _____
3. What is the estimated date of completion for this project? _____
4. What is the company's Y2K budget and have these funds been appropriately allocated?
   _____ yes ☐ no ☐
5. How long has the company's chief information officer worked with the company? _____
6. Has your company lost key information technology or operations staff in the past 12 months? yes ☐ no ☐
7. Is the year 2000 the top priority for your company?
   yes ☐ no ☐
8. Are there other information technology projects in process that may interfere with achieving Y2K certification? If yes, please detail which ones and identify business need. yes ☐ no ☐
   _____
9. Many organizations have chosen to triage mission critical systems for remediation as there is not sufficient time for a complete electronic fix to the Y2K issues. If your organization has adopted this approach:
   • What criteria were used to triage mission critical systems? _____
   • Please indicate the name and title of the person making the final triage decision. Is this person Y2K certified? _____
   • Please indicate which systems/products you deem non-critical or insignificant. (It's possible that your triage decisions will doom systems that are actually mission-critical to external and even internal dependents.) _____
   • Please indicate which products, services, information, jobs, incomes, wages, and payments on which I may depend have been condemned by your triage decisions._____
10. Does your business rely on any vendors who may adversely affect operations if there was an interruption in their ability to purchase product or provide service? If yes, what is your company doing to ensure this does not affect your ability to operate? yes ☐ no ☐
    _____
11. Did your inventory process include consideration of systems, embedded microprocessors and manual processes in the following areas:
    a) information technology? yes ☐ no ☐
    b) plant operations and facilities? yes ☐ no ☐
    c) biomedical devices? yes ☐ no ☐
    d) real estate leased, owned, and new construction? yes ☐ no ☐
    e) human resources? yes ☐ no ☐
    f) electronic commerce? yes ☐ no ☐
    g) procurement? yes ☐ no ☐
    h) public infrastructure? yes ☐ no ☐
    i) insurance? yes ☐ no ☐
    j) investments, banking, funding positions? yes ☐ no ☐
    k) transportation? yes ☐ no ☐
    l) satellite dependencies? yes ☐ no ☐
12. On what date is your organization enforcing a lock-down policy, ensuring that no date-related virus is allowed to contaminate your systems? _____
13. Has the lock-down policy and implementation date been communicated to all data sources and have these sources acknowledged your request and agreed to comply? yes ☐ no ☐
14. What certification process have you implemented to ensure receipt of only non-contaminated files?
    _____
15. Do all of your systems, devices and processes correctly recognize the Y2K as a leap year? yes ☐ no ☐
16. Do all of your systems utilize the ISO standard date format of yyyy-mm-dd? yes ☐ no ☐
17. To prevent self-inflicted virus contamination, on what date will your company enforce appropriate field naming conventions, standards, and documentation as well as require Y2K certification on all code, interface, and process walk-throughs prior to implementation?
    _____
18. Abruptly advancing a system or device date can terminate usage of the system or device as well as violate warranty and maintenance contracts/agreements. Do all of your test plans require a review of warranty and maintenance language prior to actual testing?
    yes ☐ no ☐
19. Are you continually testing your interfaces with local emergency response dispatch (911) systems, verifying that fire, law enforcement, and medical response agencies appropriately respond to your requests for assistance within the time frame recognized as standard 1/1/98? yes ☐ no ☐
20. What consideration has been given to "worst case" scenarios regarding the value-devaluation of currency and a procedure on what goods and services will be accepted in lieu of cash or credit? What is the implementation date of this procedure?
    _____
    _____
    _____

Source: Martens-West Year 2000 Consulting, Salt Lake City.

Throw away those old index cards

Standards allow applications to share patient info

An unusual thing happened one morning during grand rounds last year at Duke University Medical Center in Durham, NC, — the physicians applauded.

They had just learned of a visual integration standard called User Link. With the standard, users who have been authenticated by one application do not have to sign onto other applications on a workstation. That means they no longer have to remember the various names and passwords to sign into the different applications, information many of the physicians tote around on 3-by-5 cards. When told about User Link, they pulled out the cards from their pockets and began to applaud.

"The integration seems simple and obvious to someone who has not had to log onto multiple applications on one workstation," says **Wes Rishel**, president of Wes Rishel Consulting in Alameda, CA. People who have worked with the systems, however, know how complicated the process can be. "If you show [the standard] to people who have worked in this environment, they are very enthusiastic about it."

User Link is the latest project of the Clinical Context Object Workgroup (CCOW), of which Rishel is a member. CCOW is a consortium of health care providers and builders of information systems focusing on the collaboration among visual (graphical user interface-based, or GUI) applications on a clinical workstation.

The CCOW project began based on preliminary work from Duke, IDX Systems Corp. in Burlington, VT, and CliniEffect Systems in Durham, NC. "Duke University Medical Center has a long reputation for being successful at integrating applications," Rishel says. "[Integration] is necessary because you really can't find someone who does everything well. Even if you could, with the way that organizations are being combined, you always end up having to work with existing systems. Therefore, if a hospital buys a practice and the practice already has a system, the physicians have to use their own system and the system of the hospital, too."

Duke recognized that the ubiquity of the Windows operating system provided an opportunity to bring applications together on one workstation, he says. When users switched from one application to another, though, they had to redundantly log in or re-enter the same information.

Duke worked with IDX and CliniEffect on visually integrating the applications, and a demonstration of their efforts caught the attention of a number of health care information systems vendors at a trade show in 1996. These vendors came together as CCOW for the first time in March 1997.

More than 20 vendors and health care providers, such as 3M Health Information Systems in St. Paul, MN, and Hewlett-Packard in Palo Alto, CA, have now announced support for CCOW. **(For a list of companies with "CCOW Contributor" status, see box, p. 27.)**

"From [the first meeting] it's been a case of working out the standards and getting vendors to implement the standards," Rishel explains. "As we go forward, the idea of visually integrating these applications is the overall goal of this group."

CCOW's principles

Without an easy integration into existing GUI products, however, the goal would not succeed. That's why CCOW members have established these principles, taken from it's own white paper, to ensure that its standards would be "robust" and easily adopted:

- **Widest applicability to applications built on a GUI**. The success of a standard depends on its adoption by vendors. The larger interest is not served by building the standard around a language, development package, or piece of special software that will exclude many vendors.
- **Software component technologies.** Software technologies such as ActiveX and CORBA provide the best opportunities for robust, efficient inter-operation, and plug-and-play compatibility. Both technologies are implemented in a number of languages and development environments.
- **Low application re-engineering costs.** An explicit goal is to minimize the work that existing GUI applications would require to become compliant.
- **Plug-and-play interoperability.** Client applications should interoperate with different implementations of the context manager — an automation server that provides the services necessary to implement a context change — without a requirement for adjustments in the programming;

(Continued on page 27)

CCOW Contributors

As of September, 23 health care organizations are listed as having "Clinical Context Object Workgroup (CCOW) Contributor" status. **(To find out more about CCOW, see story, p. 22.)**

The organizations are:

- ✔ 3M Health Information Systems, St. Paul, MN
- ✔ ClinEffect Systems, Durham, NC
- ✔ Component Software International, Mason, OH
- ✔ Corechange, Boston
- ✔ Duke University Health System, Durham, NC
- ✔ Healthdyne Information Enterprises, Marietta, GA
- ✔ Health Network Venture, Downers Grove, IL
- ✔ Health Patterns, LLC, LaGrange, IL
- ✔ Health Vision, Santa Rosa, CA
- ✔ Hewlett-Packard, Palo Alto, CA
- ✔ IDX Systems Corp., Burlington, VT
- ✔ Marquette Medical Systems, Milwaukee
- ✔ Mayo Foundation, Rochester, MN
- ✔ MedicaLogic, Hillsboro, OR
- ✔ Mortara Instrument, Milwaukee
- ✔ NeoTool Development, LLC, Montrose, CO
- ✔ Oacis Healthcare Systems, San Rafael, CA
- ✔ Oceania, Redwood City, CA
- ✔ OSF HealthCare System, Peoria, IL
- ✔ Share Medical Systems Corp., Malvern, PA
- ✔ Spacelabs Medical, Redmond, WA
- ✔ Sunquest Information Systems, Tucson, AZ
- ✔ VHA, Irving, TX

(Continued from page 22)

the software should be implementable at multiple client sites without reprogramming.

• **Open participation**. Participation in the group is free, but members must commit to the work. The criteria for CCOW Contributor status is consistent attendance at meetings, participation in CCOW demonstration projects, and an intent to adopt CCOW standards.

• **Standards, not software**. CCOW does not sell or give away software that is required for CCOW compliance.

• **Trade show development schedule**. Trade shows offer the ability to coordinate many vendors and receive extra publicity, as well.

CCOW has published one standard, the Patient Link. When applications cooperate using the Patient Link, they track together on the selected patient. Users don't have to reselect the patient when switching from one application to another. "We have vendors that have modified their software to support that standard," Rishel says.

The finalized versions of the CCOW Patient Link 1.1 have been posted on the Internet. They, along with other information about CCOW, can be found at http://www.mcis.duke.edu/standards/ccow. CCOW also is reviewing the use of Patient Link for Web-based applications.

CCOW is still finalizing its User Link standard. CCOW plans to show the second prototype of User Link at the Healthcare Information and Management Systems Society conference in Atlanta in February. ■

The law: Hospitals can't delay emergency care

Take these steps to get correct payer information

Concerned that patients may not be receiving proper emergency medical care because of managed care pre-authorization requirements, the federal government will begin enforcing a "patient-dumping" prohibition to ensure immediate care, whether insurance pays or not.

As the Department of Health and Human Services Inspector General June Gibbs Brown said in a press statement, "Despite the terms of any managed care agreements, federal law requires that stabilizing medical treatment be provided in an emergency." The statute is section 1867 of the Social Security Act and also known as being part of the Emergency Medical Treatment and Active Labor Act and the Consolidated Omnibus Budget Reconciliation Act.

Sanctions imposed for violations of the anti-dumping statute include the termination of the hospital's provider agreement, and the imposition of civil money penalties — up to $50,000 per incident — against both the hospital and the physician responsible for examination, treatment, or transfer of an individual. In addition, the anti-dumping statute provides for the exclusion of the physician if the violation is gross, flagrant, or repeated.

American Hospital Association spokesman **Rick Wade** applauded the expansion of the law to the press, but he emphasized that "it's not going to solve the problem of some plans deciding that they'll use pre-authorization rules as a way not to pay hospitals."

"Many of the health maintenance organizations appear to be taking the tactic of automatic denials

on payments," agrees **Susan M. Reese**, RN, MBA, president of Palm Harbor, FL-based InfoScript. InfoScript provides management resources and consulting services related to emergency departments. "The general feeling is that [the organizations] have a hope that the hospitals will just accept the denial and move on."

Under statutory amendments enacted in the Balanced Budget Act of 1997, Medicare and Medicaid managed care plans are prohibited from requiring prior authorization for emergency services, including those that "are needed to evaluate or stabilize an emergency medical condition."[1]

Moreover, Medicare and Medicaid managed care plans are required to pay for emergency services provided to their enrollees, the statute says. The obligation to pay for emergency services is based on a "prudent layperson" standard, which means that the need for emergency services should be determined from a reasonable patient's perspective at the time of presentation of the symptoms.

Karen Ignagni, president of the American Association of Health Plans in Washington, DC, told reporters that the group's members already use that standard, but they also want to make sure patients are not seeking primary care in an emergency setting.

Obligated to emergency patients

Hospitals, however, don't have the luxury of trying to decide if the need for emergency care would fall under the prudent layperson standard. Under the statute, the obligations of Medicare-participating hospitals to individuals seeking emergency services include the following:

❒ A hospital must provide to any person who seeks emergency services an appropriate medical screening examination sufficient to determine whether he or she has an emergency medical condition, as defined by the statute. When appropriate, ancillary services routinely available at the hospital must be provided as part of the medical screening examination.

❒ If the person is determined to have an emergency medical condition, the hospital is required to stabilize the medical condition of the individual, within the staff and facilities available at the hospital, prior to discharge or transfer.

❒ If the patient's medical condition cannot be stabilized before a transfer requested by the patient (or determined to be in the patient's best interest by the responsible medical personnel), the hospital is required to follow very specific statutory requirements designed to facilitate a safe transfer to another facility.

❒ A hospital may not delay the provision of an appropriate medical screening examination or further medical examination and stabilizing medical treatment in order to inquire about the individual's method of payment or insurance status.

The key to the statute is to not delay care, Reese advises. "[The regulations] do not tell hospitals they can't get the information. They tell hospitals that they can't let this information interrupt the flow of care. You can't stop providing care for patients to find out about their insurance coverage and then proceed once you know their financial status."

The Office of the Inspector General in Washington, DC, and the Health Care Financing Administration (HCFA) in Baltimore suggest the following practices to minimize the likelihood that a hospital will violate the statute:

❒ Hospitals may not request a health plan to require prior authorization before the patient has received a medical screening examination to determine the presence or absence of an emergency medical condition or before the patient's emergency medical condition is stabilized.

❒ Hospitals should not ask patients to complete financial responsibility or advanced beneficiary notification forms prior to performing an appropriate medical screening examination.

❒ Qualified medical personnel must provide an appropriate medical screening examination to all individuals seeking emergency services.

❒ A patient inquiry about his or her obligation to pay for emergency services should be answered by someone who has been well-trained to provide information regarding potential financial liability.

Hospital staff should encourage any patient who believes that he or she may have an emergency medical condition to remain for the medical screening examination and to defer further discussion of financial responsibility issues until after the medical screening has been performed.

❒ Hospitals should follow the series of steps listed in the statute in the case of an individual choosing to withdraw his or her request for examination or treatment at the presenting hospital. These steps include making an effort to secure a written informed consent to refuse examination and treatment.

Ensuring that patients receive proper emergency care, however, shouldn't stand in the way of obtaining payment information.

"Hospitals are operating in such fear of HCFA's

regulations that they are reluctant to pursue getting information upfront from a patient," Reese says. "The hospitals fear being accused of intimidating the patient in such a fashion that the patient leaves and does not pursue requested services."

Here are some suggestions to increase the amount of information hospitals receive from patients in the emergency departments:

❒ **Place nurse triage before registration.**

In some cases, the patient is then routed back to registration after care is rendered (when the patient is treated and released) to complete the data capture process, writes Allan P. DeKaye, MBA, FHFMA, president and chief executive officer of DeKaye Consulting in Oceanside, NY, through his company's Patient Accounts Management list server. Many emergency departments also fax over notifications, or have patients or staff call the managed care company to ensure that this requirement is being met, he adds.

❒ **Offer bedside registration.**

With bedside registration, clinical professionals can continue providing uninterrupted clinical care while registration personnel can pursue getting the demographic and financial information, Reese says.

❒ **Work on customer relations.**

Registration departments can do a better job in terms of customer relations so that the process is not adversarial, she says. "Some patients see it that way and think they are being challenged."

❒ **Have a more knowledgeable registration staff.**

"That's a tall order with all of the variety of financial plans available for patients," Reese admits. "Oftentimes, though, one of the problems in obtaining the correct information is that the registrar does not know the types of plans and what information might be required by them."

❒ **Put financial counselors into emergency departments.**

"Oftentimes, patients who come into the emergency department don't understand their plans," she says. "Or they don't have a plan but they qualify for other aid but don't know it because no one has ever pursued getting it for them. Financial counselors could assist those individuals to evaluate what their financial package is and help find payment sources for them."

Reference

1. 63 *Fed Reg* 67,486 (Dec. 7, 1998). ■

Are you prepared if Y2K delays HCFA payments?

The check's in the mail

Reports have been flying out of Washington that the Health Care Financing Administration (HCFA) in Baltimore is woefully unprepared for updating its systems to comply with the year 2000 (Y2K) transition.

Last September, the technology subcommittee for the U.S. House Government Reform and Oversight Committee gave the Department of Health and Human Services an "F" for its efforts to fix the Y2K problem. Then a report published by the General Accounting Office (GAO) in Washington said that HCFA's repairs lag far behind schedule.[1]

"Because of the magnitude of the tasks ahead and the limited time remaining, it is unlikely that all of the Medicare systems will be compliant in time to guarantee uninterrupted benefits and services into the year 2000," the report says.

HCFA, however, is singing a different tune. HCFA's chief information officer Gary G. Christoph, PhD, is on record saying that all internal mission critical systems will be repaired and tested by Dec. 31, 1998, says **Glenn M. Pearl**, MHSA, editor of *Rate Controls* newsletter, a statistical and opinion resource for hospital chief financial officers in Phoenix.

HCFA has more than 50 million lines of code to revise in its 99 mission critical systems. "[Christoph] is saying that 95% of code has been revised for external systems — the intermediaries and contractors," Pearl says. Christoph even indicated that HCFA is now less inclined to provide additional payments in late 1999 to prevent disruptions in cash flows.

"You can see there are divergent views between what Congress is being told and what HCFA is reporting at this point," Pearl adds.

Although Christoph has indicated that HCFA's Y2K compliance efforts are more on schedule than what other government sources report, most contingency planning experts say HIM professionals should prepare for all scenarios — including the possibility that HCFA system problems could disrupt cash flow in the year 2000.

Here are some steps hospital financial personnel can take to prepare for a possible disruption in cash flow in the year 2000:

• **Conduct a cash flow analysis.**

This analysis will help hospital financial personnel know how much cash is needed per day, says **Frank Tucker**, president of Catalina Software in Dana Point, CA.

Next, the personnel have to estimate how much HCFA might disrupt cash flow if the government interrupts benefits for a period of time after the turn of the century. Armed with the knowledge of how much cash is needed by their hospital per day, financial personnel can better estimate how much cash they need to get through that time.

• **Don't neglect any cost centers.**

"You need to make arrangements for every area where cash is needed," Tucker says. "Decide what you are going to do in each area and how you are going to cover the cash flow disruptions for each."

• **Investigate your state payroll laws.**

Some hospitals may decide to delay employee payroll for a few days to ease their cash flow problem. They should consult their legal counsel first because it may result in penalties from the state. "Some states have strict laws on meeting payroll," he says.

• **Keep everyone informed.**

Vendors need to be advised about possible temporary disruptions in cash flow so delivery of goods won't be stopped if payments are late, Tucker says. "Everything should be worked out ahead of time.

"The sooner and the more you keep people informed of a cash flow problem, the better chance you have of getting through it. If you're not talking to your suppliers and your employees, then real problems may develop."

• **Consider lines of credit.**

Lines of credit from financial institutions can help cover a temporary cash crisis, he says. Given the possibility that a bank may also experience some Y2K difficulty, however, hospitals may want to pursue lines of credit from several different financial institutions.

Hospitals don't only have to turn to outside sources for extra cash. They also can attempt to warehouse cash by reducing their receivables, advises **Allan P. DeKaye**, MBA, FHFMA, president and CEO of DeKaye Consulting in Oceanside, NY.

"If you start accelerating your work now to get to a lower receivables level, you'll create more cushion now, he says. "You don't want to get fatter with your receivables; you want to get leaner. It's like losing weight before you go on a cruise. You take off some weight because you know you're going to gain some on the trip."

Hospitals should start a process of accounts receivable management and reduction, he says. "It's something you should be doing anyway, but people play to averages and don't necessarily try to take receivables down to a much lower level."

To say "60 days in accounts receivable" usually means a payment in 60 days is the average, DeKaye says. "To me that means anywhere from 40 to 80 days. You certainly want to bring down the payer who is paying you in 80 days to your average of 60."

An average of 60 days also is not adequate if creditors are asking for payment in 45 days. "[Hospitals] need to set reasonable targets that should be both related to what is normal for the industry and their case mix, and to their budgetary requirements," he explains.

Who pays the fastest?

One tool DeKaye likes to recommend is for providers to look at which payer is the most prompt in its payments. "Are you actually getting paid in the minimum amount of time from that payer?" he asks. "For example, Medicare has a two-week holding period. Is Medicare paying you 14 days after you submit a claim?"

As another example, providers may have a managed care contract that specifies payment in 30 days from the date of "clean claim" — the date a claim is submitted with all the correct information. "If payment is in 40 days, what was wrong with your claim that you didn't get paid in 30 days? If you left off some information, then it's your fault. But if they were slow on the uptake, fault them."

Many providers are content with the time period that they receive payment, even though it may take longer than what is stated in the contract. "Why have a contract then?" DeKaye asks. "You have to know that you're not getting paid when you should. Some providers don't check at all."

Providers can call payers to ask about the payment periods, or better yet, they can visit the payers' offices." Many times providers are not as aggressive to say hello," he says. "[They can say], 'I'm coming to your office and would like a check ready for me for the claims I have sent you.' Or 'I am coming to your office and want to review the accounts not being paid. If you don't pay me, you're going to be in default of your contract.'"

Most providers, though, aren't that aggressive because they fear losing the contract, DeKaye says. "This may mean there should be more safeguards, such as performance guarantees, in the contract.

"People shouldn't use Y2K as a reason to lower their investment in receivables," he concludes. "They should lower their investment in receivables because it is good business sense."

Editor's note: Contact DeKaye Consulting on its Web site: http://www.dekaye.com, e-mail: adkcmpa@aol, or call (516) 678-2754.

Reference

1. General Accounting Office. *Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy*. GAO/AIMD-98-284. Washington, DC; September 1998. ■

NEWS BRIEFS

HCFA releases final Internet policy

The Health Care Financing Administration (HCFA) in Baltimore issued a bulletin on Nov. 24, 1998, that formalized its policy and guidelines for the security and appropriate use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. The Internet policy covers all systems or processes that use the Internet, or interface with the Internet, to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information, including Virtual Private Network and tunneling implementations over the Internet. Non-Internet Medicare/Medicaid data communications processes (such as use of private or value-added networks) are not changed or affected by the Internet policy.

HCFA finds minimally acceptable a level of encryption protection equivalent to that provided by an algorithm such as Triple 56-bit DES (defined as 112-bit equivalent) for symmetric encryption, 1,024-bit algorithms for asymmetric systems, and 160 bits for the emerging elliptical curve systems, as of November 1998.

As stated in the policy, HCFA reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption, such as a brute-force exhaustive search.

(For more information about HCFA's draft Internet policy, see *Hospital Payment & Information Management*, November 1998, p. 163.)

To view HCFA's final policy, visit the Web site at http://www.hcfa.gov/security/isecplcy.html. ▼

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 $83 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.

AHA asks HCFA to delay physician fee start-up

In a December letter, the American Hospital Association (AHA) in Washington, DC, asked the Health Care Financing Administration (HCFA) in Baltimore to delay the effective date for payment to hospitals under the physician fee schedule. The date was slated for Jan. 1, 1999.

The schedule was published in the *Federal Register* on Nov. 2, 1998.[1]

"Switching from payment on a reasonable cost basis to the fee schedule will require major coding and billing system changes, and to date, HCFA has failed to notify hospitals of these requirements," wrote Rick Pollack, AHA's executive vice president of government and public affairs.

"Fiscal intermediaries, generally unfamiliar with the procedure and revenue codes associated with the fee schedule, have not provided hospitals with lists of codes and payments associated with these [outpatient] therapies."

Other delays

HCFA has already announced that system modifications required for outpatient prospective, also scheduled for a Jan. 1, 1999, start-up date, will be delayed.

Since the time frame for changes required for that conversion were thought to correspond to system changes required for the fee schedule, Pollack asked for the payment to hospitals for outpatient therapies be delayed as well.

Reference

1. 63 *Fed Reg* 58,813 (Nov. 2, 1998). ▼

JHITA reviews comments on HIPAA standards

The Joint Healthcare Information Technology Alliance (JHITA) has reviewed the comments for the Department of Health and Human Services' (HHS) proposed rule on security and electronic signature transactions. The standards were mandated under the Health Insurance Portability and Accountability Act of 1996.

The comments have been posted on the Administration Simplification Web site at http://aspe.os.dhhs.gov/admnsimp/.

"It is clear that health care providers and organizations are asking the HHS [in Washington, DC] to provide more direction in implementing the provision during the writing of the final rule," JHITA states. Most of the comments submitted came from insurance companies, state government offices, consumer organizations, and advisory committees.

The comments on the proposed rule expressed concerns about the following:

❒ The proposed rule does not say how it will be implemented in light of privacy legislation expected to come from Congress.

❒ The rule is not clear about what it specifically requires.

❒ The rule only sets forth procedures and does not establish any specific standards to ensure the security of health care information.

❒ The rule does not set forth any penalties for not complying with the procedures.

❒ The rule needs additional definitions, such as "agents" of health plans.

❒ The rule provides specific requirements that were overly excessive or restrictive.

❒ The rule does not classify telephone, voice mail or fax transmissions as electronic transactions, although they are the most common ways organizations share information. ■