HIM Survival Kit for the Year 2000

by Elizabeth Wheeler, RHIA (formerly RRA)

Is your organization ready for the Year 2000? The "millennium bug" offers some useful lessons in risk assessment. Here's how to build a contingency plan to ensure business continuity on January 1, 2000.

The information technology (IT) field may have generated Year 2000 concerns, but planning to avoid business failures in the new millennium is not just an IT issue -- it's a broad-spectrum business issue. There are numerous potential points of failure beyond a malfunctioning piece of hardware or software. To meet the challenges of Y2K, regardless of their origin, it is critical for health information management (HIM) professionals to become aware of the risk assessment process. This process involves having an intimate knowledge of the mega processes of their workplace, documenting the major processes of the business units for which they are responsible, and identifying existing interdependencies and recognizing their potential impact on the HIM department. HIM professionals must also understand the vital role contingency planning may play in ensuring business continuity on January 1, 2000.

A Planning Primer

Q: What exactly is contingency planning? How is it different from business continuity?

A contingency plan is an action plan put in place before a disaster occurs. In this case, the century date change is the "disaster" that may result in business process failures. Contingency plans anticipate failures and establish procedures that will allow a department's business processes to continue. The good news with Y2K issues is that we know what to expect and we know when to expect it. However, without a fully developed contingency plan in place, the impact can vary from insignificant to insurmountable.

A contingency plan prompts managers to explore various "what if" scenarios. An example: On January 1, 2000, the medical staff is unable to use the hospital's telephone system to dictate medical reports. Is there a backup system for dictation using tape recorders? Will the staff be able to produce handwritten reports in a timely manner and maintain the degree of quality required by regulatory agencies? Further, because of the failure of the telephone system, transcribed reports cannot be sent back to the hospital over a modem. What is the contingency plan for getting the patients' medical information and care plans to the caregivers?

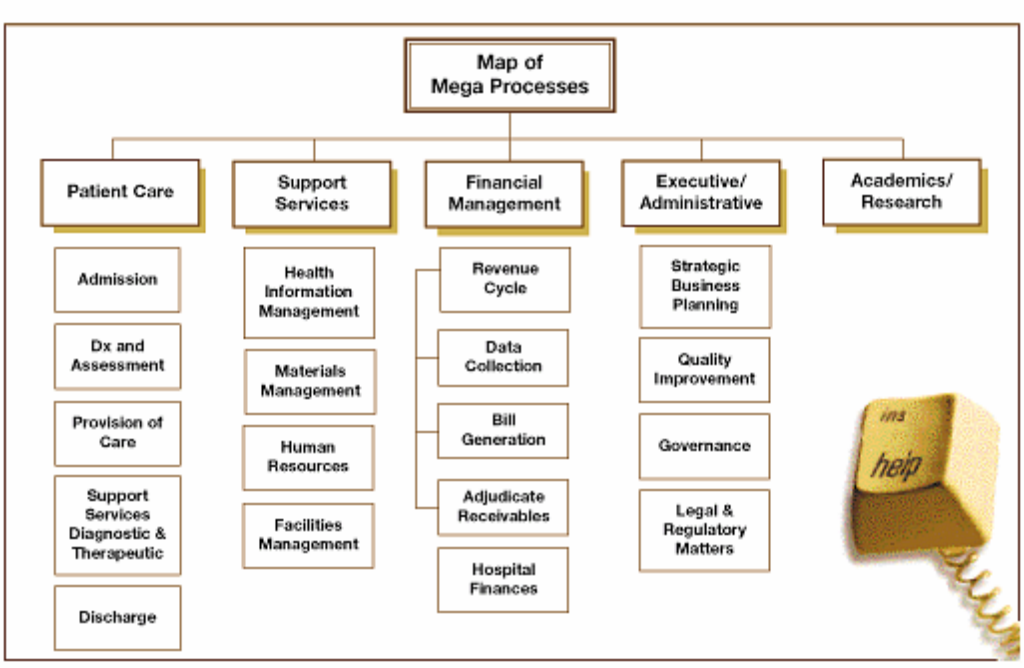
From this example, you can see the value of a well- constructed contingency plan. If the telephone system fails on 1/1/2000, policies and procedures will be in place to help ensure that medical data continues to be collected and documented for all patient care situations. In other words, business continuity has virtually been guaranteed.

Q: How do I create contingency plans for the HIM department?

The head of the HIM department should be responsible for ensuring that contingency plans exist for this business unit.

Start by documenting every business process occurring throughout the department. Business processes are the activities or functions performed within the department that support the organization's mega processes, such as direct patient care, indirect patient care support, administration, financial management, academics, or research (see Figure 1). To identify each function, refer to the department policies and procedures manual or a list of HIM staff job titles.

Figure 1: healthcare mega process map



Typical major business processes of the HIM department include:

- support functions, such as filing and retrieval of medical records, assembly of discharged records, preparation of folders to house records, printing reports
- filing loose reports such as ancillary test results
- receiving and printing transcribed reports or transcribing dictated reports in-house and filing reports in medical records
- analyzing medical records for deficiencies and creating deficiency analysis reports
- coding diagnoses and procedures
- abstracting data from medical records
- processing requests for release of information from medical records
- submitting data to registries and databases
- administrative management of the department

List all tasks performed for each business process. Document the systems (hardware, software, and interfaces) and vendors that play a role in each task when it is performed in the usual and customary fashion. Assess each dependency individually, assuming it will fail. Then develop a contingency plan that will maintain a smooth flow of tasks or information until the failed system is restored to proper functionality.

Once the HIM department's major business processes and system dependencies have been documented, risk assessment can be performed. To do this, assign a severity and an exposure rating to each process and dependency or dependent inventory item. This rating scale may be any arbitrary scale the organization designs; however, all departments within the organization should use the same scale (see "Sample Risk Rating Table").

Sample Risk Rating Table for Severity and Exposure

Rating	Severity of Risk	Potential Exposure
High (3)	• Patient care is disrupted	• Organization's mission is substantially impeded

	• Breach of data integrity, loss of critical data, system interruption or failure • Sensitive data exposed (due to failure of security mechanisms)	• Invalid data analysis or interpretation, data corruption • Unable to acquire products or services
Moderate (2)	• Failure of noncritical healthcare delivery system • Diminished systems or data integrity (can be identified and corrected with significant effort)	• Timeliness of mission-related decisions and actions is affected • Resource management is hindered • Large costs to detect and correct problems • Strain on good working relations
Minimal (1)	• Personal or group productivity interrupted • Issues with systems or data integrity are apparent and easily corrected • No risk to delivery of patient care or confidentiality	• Non-catastrophic system problems with limited scope are detected • No effect on mission, fiduciary, or legal systems • Increased stress among staff

Now you have reviewed your department's major business processes, you have identified the inventory items needed to support those processes, and you have assessed the severity of the risks should a product or system fail. Next, you need to consider the HIM department's external suppliers and trading partners. Query your outside suppliers regarding their Year 2000 compliance planning efforts and identify potential points of failure with these business partners.

Business Preparation Is Simple
Do a self-assessment: Document inventory and gather compliance data
Be proactive: Initiate actions to identify inventory and departmental business processes, assess risk, and develop contingency plans
Stay informed: Use the Internet to collect current information on compliance status and product testing
Test and drill: Put the contingency plan into action before it is needed

Take a Test Drive

With a contingency plan in place for every potential disruption to your department's business continuity, advise your staff of the contingency plans and train them to implement the plans. Test the plans -- and preparedness of your staff -- by running a drill. For instance, if your plan to code diagnoses and procedures relies on the return to a manual process, this may not be easily executed.

Using a manual backup for processes routinely performed electronically doubtlessly will require more resources in terms of personnel and time. What is the skill level of your coding staff? When was the last time they used coding books rather than an encoder? Does your coding unit have reference books for coding advice, or does your staff rely on help references that are built into the software? Does your department have a set of code books for each staff member? Will a larger coding staff be required to maintain a coding rate that will not negatively impact the organization's accounts receivables? Test your manual coding contingency plan and determine whether you need to conduct training sessions, hire more people, or draft a new plan.

Whether you are writing contingency plans for the first time or you are revising a plan that has been tested, prepare an estimate of the cost of executing the contingency plan. Evaluate to see if less expensive alternatives exist to maintain business continuity.

Take Action Now

Contact all of your hardware, software, and interface vendors now to obtain free product upgrades. Request an upgrade to the compliant version or replace the product before the Year 2000. It is critical to be on the vendor's installation schedule early to

allow enough time for testing. And keep in mind that the replacement or upgrade of a system does not eliminate the need for contingency plans.

Elizabeth Wheeler *is a management consultant with Superior Consultant Company, Inc., and past president of the New York Health Information Management Association.*

Article citation:
Wheeler, Elizabeth. "An HIM Survival Kit for the Year 2000." *Journal of AHIMA* 70, no.2 (1999): 46-48.
