INSURING HOSPITALS AGAINST THE Y2K BUG: WHAT RISK MANAGERS NEED TO KNOW

Peter Flattery, Hospital Insurance Reciprocal of Canada (HIROC)

Most insurance companies have by now declared their position with respect to coverage for the Year 2000 (Y2K) problem. Few are providing full coverage, though property insurers are providing significant protection for resultant damage claims. Liability insurers are generally avoiding coverage.

In this article I will attempt to explain the dilemma that insurance companies face regarding coverage as well as their response to the Y2K exposure, Y2K insurance products and the steps hospitals can take to reduce their exposure.

In an effort to attract attention to the potential for enormous damages that could be caused by the Y2K problem, a United States senator referred to the Y2K as “The Asteroid.” The vision of an asteroid heading toward earth is certainly more of an attention-grabber than a “bug” inside a computer system.

**Insurers’ Position**

Is the Y2K problem insurable?

Insurance policies are designed to respond to events that are unexpected or unintended from the standpoint of the insured (this is the principle of fortuity). We all know about the Y2K problem – it is in the newspapers and magazines, is discussed at work, and so on. It is a foreseeable event and, therefore, not covered according to the insurance industry in general. Industry experts estimate it will cost in the hundreds of billions of dollars to fix the problem.

Most insurers are reluctant to insure the Y2K problem. It is a very difficult exposure for insurers to quantify since no one fully understands the breadth of damage that could be caused by the failure of computer systems or embedded chips. Without a reasonably accurate appreciation of the potential of loss costs, actuaries cannot determine appropriate premium levels.

Some insurers will do nothing, remaining silent on the issue of coverage and relying on the principle of fortuity to deny coverage outright. Other insurers will add Y2K exclusions by endorsements to policies rather than rely solely on the fortuity argument. References to the “Year 2000” do not appear on such exclusions because computer-system malfunctions could occur before and after January 1, 2000. Instead, insurers are more apt to make reference to “Misinterpretation of Date(s)” when describing the issue.

Adding exclusions, however, could trigger the reporting of claims by policyholders. It could be interpreted by the insured that coverage must have existed before the exclusion was adopted. Insurers are taking a chance that claims will be reported if exclusions are added.

There are two general areas of insurance coverage (or lack thereof) that could affect hospitals – property (including boiler and machinery) and liability.

**Property Insurance**

Generally speaking, property insurers of hospitals are adopting the Insurance Bureau of Canada’s suggested exclusions or modified versions thereof. The exclusions apply to damage caused to the actual unit encompassing the computer

Adding exclusions, however, could trigger the reporting of claims by policyholders.
Some predictions from major industry analysts:

The Gartner Group estimates that converting computer systems to handle 21st century date information will cost $400 - $600 billion world-wide. Software Productivity Research, Inc. puts the total cost, including software, hardware and database repairs, plus litigation expenses and damage awards, at $1.635 trillion. Money aside, industry analysts agree that there is little likelihood that serious Year 2000 failures can be avoided entirely. Gartner Group estimates that 25% - 50% of all computerized organizations will not achieve full Year 2000 compliance in time. A Standish Group International study reports that more than 90% of all IT projects are delivered late or never completed.

Table 1

<table>
<thead>
<tr>
<th>Type of Policy</th>
<th>Hospitals</th>
<th>Specific Y2K Exclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Liability</td>
<td>High</td>
<td>Recommended</td>
</tr>
<tr>
<td>Product Liability</td>
<td>Low</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Professional Liability</td>
<td>High</td>
<td>Recommended</td>
</tr>
<tr>
<td>Directors &amp; Officers’</td>
<td>Very High</td>
<td>Compulsory</td>
</tr>
</tbody>
</table>

While the reinsurer maintained the document was for discussion purposes only, it does offer a glimpse of how at least one reinsurer is approaching the Y2K problem. This document was distributed to many insurers and reinsurers and may have influenced the position taken by a number of underwriters.

Hospitals' Position

Hospitals can reduce their exposure to the Y2K problem by obtaining insurance, repairing/replace/removing from service non-compliant equipment and systems, or a combination of all three. After reading the insurer's position it may appear unlikely that coverage for liability exposure is available. Hospitals that have not already done so should ask their insurer what coverage is available to them.

Healthcare Insurance Reciprocal of Canada (HIROC) has included a Y2K exclusion with its January 1, 1999 renewal. Coverage is available, however, for bodily injury and professional liability to all its member hospitals provided they meet the following criteria: (I have included HIROC’s position in this section rather than in the “Insurer’s Position” section because HIROC is a hospital-owned insurer and, therefore, a hospital-generated solution to the Y2K problem.)

1. Completion of an inventory listing of all systems critical to the provision of healthcare services;
2. Identification of those critical systems that could be negatively impacted by the misinterpretation of dates; and
3. Confirmation that those critical systems identified in item 2 have been tested for the misinterpretation of dates. (HIROC understands that some vendors, particularly those involved with large equipment such as CT scanners and MRIs, request that hospitals

DID YOU KNOW...

Some predictions from major industry analysts:

According to the Information Technology Association of Canada, “It may now be too late to completely remediate the Y2K problem. Contingency planning is the next best line of defense.”
There are no guarantees that a fully compliant system will not break down, regardless of testing or vendor assurances.

4. Confirmation that all those critical systems identified in item 2 interpret dates correctly.

5. A formal contingency plan is in place if systems fail owing to the unanticipated misinterpretation of dates.

The criteria are directed specifically toward systems critical to the provision of healthcare services because patients would be most vulnerable because of a Y2K breakdown of equipment. HIROC believes that patient safety is of primary concern to hospitals and that it could potentially be the greatest source of claims against hospitals.

Even if a hospital believes it is fully Y2K compliant, insurance coverage is very important for three reasons:

1. There are no guarantees that a fully compliant system will not break down, regardless of testing or vendor assurances.
2. If vendor-tested and approved equipment turns out to be non-compliant and the hospital is named in a suit alleging damages, the vendor may not have Y2K coverage and could declare bankruptcy.
3. Defense costs could be very expensive should claims be received by a hospital alleging injury caused by a Y2K problem.

If a claim is submitted by a HIROC hospital and the hospital has confirmed it has met the stated criteria, HIROC will provide coverage.

It may come as no surprise to some that a hospital-owned insurer is offering Y2K coverage. HIROC, however, has to persuade reinsurers that its risk-management approach to Y2K is sound before they would agree to participate. It is also worth noting that, in general, HIROC hospitals would only support HIROC’s position based on formal confirmation of individual hospital compliance.

Even if a hospital believes it is fully Y2K compliant, insurance coverage is very important for three reasons:

1. There are no guarantees that a fully compliant system will not break down, regardless of testing or vendor assurances.
2. If vendor-tested and approved equipment turns out to be non-compliant and the hospital is named in a suit alleging damages, the vendor may not have Y2K coverage and could declare bankruptcy.
3. Defense costs could be very expensive should claims be received by a hospital alleging injury caused by a Y2K problem.

If a claim is submitted by a HIROC hospital and the hospital has confirmed it has met the stated criteria, HIROC will defend and pay damages, if any. We will require documented evidence of the hospital’s compliance.

Example: A patient is receiving intravenous morphine. On January 1, 2000 a non-Y2K compliant chip in the IV infusion pump allows free flow of the morphine. As a result, the patient ends up in a coma. The patient’s family sue. If the hospital can demonstrate that the infusion pump was tested, and had passed the Y2K compliance test, HIROC will provide coverage.

It may come as no surprise to some that a hospital-owned insurer is offering Y2K coverage. HIROC, however, has to persuade reinsurers that its risk-management approach to Y2K is sound before they would agree to participate. It is also worth noting that, in general, HIROC hospitals would only support HIROC’s position based on formal confirmation of individual hospital compliance.

(Peter Flattery is Attorney and Chief Executive Officer of Healthcare Insurance Reciprocal of Canada (HIROC), a leading provider of general and professional liability and risk-management services to Canadian healthcare organizations.)

Assessing Business and Legal Risks of Y2K in Hospitals

The Boston law firm, Cosgrove, Eisenberg & Kiley, suggests hospitals take the following steps to assess their Y2K business and legal risks and develop comprehensive compliance plans.

A business risk assessment should first inventory internal information technology systems, as well as embedded chips and third-party dependencies. The inventory should be cross-referenced to the patient services, projects and business functions the technology supports. Potential system failures should then be evaluated in terms of expected timing, consequences and criticality.

A Year 2000 legal audit should inventory and evaluate existing contractual and other legal rights, obligations and remedies as they relate to the identified business risks, particularly those that are high-risk and mission-critical. The dual objectives of the legal audit are to determine whether vendors, service providers, insurers or other third parties might be responsible for correcting certain Y2K problems or bearing some or all of the cost, and to identify where the hospital and its officers might face legal exposure.

A due diligence plan along the following lines should then be developed and managed aggressively:

• track third-party compliance efforts;
• develop Y2K contracting and purchasing policies;
• prepare contingency and disaster recovery plans;
• disclose material Year 2000 contingent liabilities, as may be required;
• notify insurers of potential claims;
• document compliance efforts;
• prepare for litigation by and against the hospital; and
• provide directors and officers with information they need to comply with fiduciary duties and regulatory responsibilities.

The complete article can be found on the World Wide Web at: www.2000legal.com