

Ohio State Board of Pharmacy

Year 2000 Information Pack:

Suggestions

To Assess and Correct Y2K Issues

To Ensure Patient Care and Business Continuity

Intended Audience:

Pharmacists,

Pharmacies,

And

Other Health Care Provider Sites and Professionals

FOREWORD

This document is issued solely to familiarize the reader with some of the potential problems associated with the coming of the year 2000 and ways in which Ohio health care providers, pharmacies, and pharmaceutical supply organizations might prepare for their solution.

It provides a broad range of suggestions and discussion. As such, recipients are entirely responsible for taking action appropriate to their own organizations and for any consequences of such actions. The Ohio State Board of Pharmacy, the State of Ohio, and its agents cannot be held responsible for any loss or damage as a result of following the suggestions given in this document, neither can they be held responsible for any problems that may occur despite following these suggestions. If readers are in any doubt about how this information should be applied, they should consult a suitably qualified professional adviser.

The dialogue provided in this document reflects best practices derived from multiple sources within the industry and the health care community as a whole when the document was written, and may not reflect current best practices.

The State of Ohio, its officers, employees and agents (on behalf of whom this notice is issued) shall be under no liability or responsibility in negligence or otherwise to any person in respect of any inaccuracy herein or omission herefrom, or in respect of any act or omission which is caused by or contributed to this report being issued with the information or dialogue it contains.

This document is derived from several public domain sources and may only be used for personal or private organizational use. It may be copied and distributed as necessary to provide the greatest awareness within the industry targeted. It may not be sold for profit or other gain.

TABLE OF CONTENTS

1.	INTRODUCTION.....	1
1.1	Background	1
1.2	Purpose of Document.....	1
1.3	Structure of Document.....	1
1.4	References	2
2.	NATURE OF PROBLEM.....	3
2.1	The Year 2000 Date Problem	3
2.2	How Serious is It?.....	4
2.3	What are the Sources of the Problem?	5
2.4	Characteristics of the Problem.....	6
2.5	Linked Systems	7
3.	AN APPROACH TO SOLVING THE PROBLEM	8
3.1	Awareness.....	8
3.2	Inventory/Audit.....	8
3.3	Analysis	9
3.4	Remediation/Action	10
3.5	Clean Management of New Systems.....	10
4.	INVENTORY/AUDIT.....	11
4.1	Inventory	11
4.2	Related Documentation	12
5.	ANALYSIS	13
5.1	Supplier Contact.....	13
5.2	Assessing Supplier Responses	16
5.3	Impact Analysis.....	16
5.4	Testing.....	17
5.5	Inventory and Analysis Report.....	18
5.6	External Assistance	19
6.	REMEDIATION/ACTION.....	20
6.1	Replace It	20
6.2	Ignore It	21
6.3	Fix It.....	21
6.4	Work-around It.....	21
6.5	Revert to Manual Operation.....	21
6.6	Contingency Planning.....	22
6.7	Ownership Considerations.....	22
6.8	Supply Chain Considerations	23
	APPENDIX A - THE INDEPENDENT RX PHARMACY	A.1

1. INTRODUCTION

1.1 Background

The responsibility for successfully resolving the Year 2000 issues within a pharmacy or other health care provider site resides with the entity itself.

Recognizing that there are a significant number of issues involved in this process, the State of Ohio Year 2000 Competency Center, at the request of the Ohio State Board of Pharmacy, drafted this information booklet concerning the Year 2000 issues that may affect a pharmacy or other health care provider site as licensed in the State of Ohio. It was determined, based on experience and a review of the data available, that a representative or *sample* retail pharmacy practice, called *The Independent Rx*, be a model for this document. This model would identify key failure areas that the typical retail pharmacy would encounter in relation to the Year 2000 and the corresponding date-related issues. The aim of this work is to produce information and suggestions that can be disseminated and applied to all Ohio pharmacies/health care provider sites.

1.2 Purpose Of Document

These notes provide a broad range of suggestions on tackling the Year 2000 problem within each health care provider entity. The notes concentrate on the key areas of:

- Identification and recognition of systems with potential for Year 2000 related problems
- Inventory, Audit and Analysis of problem systems
- Role of the supplier/manufacturer

Each health care provider site has distinct issues that must be addressed along with the global issues of any pharmacy/health care provider site. A number of systems and equipment types utilized in providing health care are documented with an explanation of why they are considered potentially at risk from the Year 2000 problem.

1.3 Structure Of Document

Section 1 (this section) gives an introduction to the document, the purpose and structure of the document, the scope of the document, and a list of references made.

Section 2 gives some background into the cause of the problem and its characteristics.

Section 3 describes a 'five step approach' to solving the problem.

Section 4 describes in some detail how an inventory should be performed.

Section 5 describes the various steps involved in the analysis stage of the Year 2000 program.

Section 6 deals with the approach that may be taken to resolve the actions that will arise out of the aforementioned stages.

Appendix A presents the findings of a Year 2000 analysis of a typical independent retail pharmacy, *The Independent Rx*.

1.4 References

Ohio Guidebook 2000, The Year 2000 Problem

2. NATURE OF PROBLEM

The Year 2000 problem has received a great deal of publicity in recent months. Opinions differ as to how much trouble will be caused, but there is little doubt that health care providers will be affected.

This section introduces the Year 2000 problem and identifies its root causes. We explore how the existence of the Year 2000 problem is likely to have an impact on all health care provider sites, including pharmacies.

2.1 The Year 2000 Date Problem

The root of the problem lies in the common usage of only two digits to identify the year portion of a date (e.g., 10/21/98) rather than four digits to include the century as part of the date (e.g., 10/21/1998). This is a widespread action and has been used for many years by manufacturers, programmers, and users of computer systems.

As a result, many operating systems, packages, and applications now use two-digit year fields to determine time, and to perform time-based calculations. At the Year 2000, systems and software based on this approach will identify the year as "00", which in many systems relates to "1900", with the result that an event occurring in 1999 will be calculated as having happened 99 years ago ("00" - "99"). Calculations will go awry, systems may fail, and whole processes may be affected.

Most problems occur when dates after the start of the year 2000 must be entered (e.g., 3/6/00). The computer cannot tell if this refers to the century of 1900 or 2000 and in most cases will assume 1900. Problems that have already arisen because of this are:

- Booking systems have been unable to accept appointments beyond 1 January 2000.
- A pharmaceutical manufacturer began destroying a new batch of medicines as they rolled off the labelling machine due to a "00" expiration date which was perceived to be over 97 years old. The problem was identified only after unusual increases in automated replacement stock ordering triggered alarms.
- Supermarket stock control systems have rejected cans of processed meats with a sell by date in "00" as being 97 years too old.
- Credit cards with an expiration date in the year "00" are deemed to have expired or cause the Point of Sale system to lock up and prevent further processing.

The effects are not confined to computers but may appear in almost any equipment containing electronic chips (microprocessors), such as:

- Telephone switchboards.
- Security access systems.
- Medical equipment such as ultrasound or ECG machines.

These are the most readily recognized "Year 2000" problems, but readers should be aware that there is a more general problem associated with what is called "date discontinuity". Date discontinuity occurs when the time as expressed by a system or its software does not successfully move forward in line with true time.

For instance, the clocks of some systems calculate time as an offset from a fixed point (i.e., number of clock ticks since a fixed time and date). When the register counting these clock ticks overflows, the register will revert to 0, and the system clock will revert to its fixed origin date. There are a variety of systems based on this principle.

There is also a special case associated with the fact that the Year 2000 is a leap year. Some systems and applications are incorrectly programmed in this regard, and risk failure at 29 February 2000 or 31 December 2000 (the 366th day of the year).

In reading this document, please assume that the information provided for the "Year 2000" problem should be applied with equal concern to handling other date discontinuity problems.

2.2 How Serious Is It?

The Year 2000 problem has frequently been misreported as affecting only large, old systems or mainframe computers. While it is true that organizations face major difficulties with older systems, the majority of PCs and small systems also have problems. The most significant problems for health care providers are likely to be:

- Dispensing systems, practice systems, and call/recall systems may not function properly. For example, the booking of appointments after 1/1/2000 may not be possible. Most suppliers have now written to their customers explaining their policy on the Year 2000, but upgrades to the software may be required. These may in turn necessitate upgrades to the hardware. Some suppliers are not yet clear how their systems may be affected.
- Business systems such as accounting packages, payroll, or call logging software may be affected. Many suppliers have now announced their policy on solving the problems, but upgrades may be required.
- Homegrown software such as spreadsheets or database systems may be affected. The effects are worse if you have used 2-digit years (e.g., 12/01/25). You may need to change your data to use 4-digit years (e.g., 12/01/1925). You may also have to upgrade to a later version of the software package. If you upgrade to a later version, be aware that 2-digit years may be treated incorrectly (e.g., 12/01/25 may be displayed as 12/01/2025 rather than 12/01/1925). Rather than risk using 2-digit years, you should change to 4-digit years whenever possible. Bear in mind that this may necessitate the conversion of historical data as well.
- Date rollover on PCs. For relatively small organizations solving this should be relatively easy compared to problems mentioned above.
- Computer operating systems - the basic software that makes the computer work - may not work correctly. The common PC operating systems, MS-DOS, Windows 3.1 and 3.11, have documented problems. Windows 95 and Windows 98 are hardly affected but there will be some problems still with software written specifically for these operating systems. Some versions of BOS, UNIX, and XENIX may also have problems. In most cases the system supplier can solve these in a straightforward manner, normally by installing the latest version of the operating system.

In summary, the effects of Year 2000 are difficult to predict but range from minor inconveniences to a total inability of the health care provider to function.

2.3 What Are The Sources Of The Problem?

There are several ways in which the Year 2000 problem can appear at a health care provider site, for example:

- Systems will not accept or process any dates beyond the end of 1999.
- Computer clocks fail to move from 12/31/1999 to 1/1/2000. This is usually known as the "date rollover problem". It affects most PCs and embedded systems.
- Systems do not recognize Year 2000 as a leap year. They may either calculate time period incorrectly or fail to work at all on 2/29/2000.
- Critical diagnosis or dialysis equipment fails to work as the internal calibration date registers as over 99 years out of date.

Some equipment, both medical devices and non-medical devices, contain embedded microprocessor chips which, should they fail, could cause chaos at any health care provider site (e.g., telephone switchboard, in-hospital paging, Intensive Care Monitoring equipment, drug infusion pumps, etc.).

Listed below is a selection of systems and equipment items that may show problems with the Year 2000. Not all will necessarily apply to each health care provider site. The list is neither complete nor definitive.

Software Systems

Clinical systems
Accounting systems
Automated Drug Dispensing systems
Financial, personnel, payroll, and other business systems
Call and recall systems
Records Management systems

Communications Links

Links to Health Authorities/Security Providers
Links to providers - path lab & discharge
Registration/Items of Service links
EDI/on-line banking systems

Software

Spreadsheets
Word processing and Desktop Processing
Databases
Operating systems
Bar Code Systems

Hardware

PCs, file servers, and workstations
Hand-held computers/organizers
Laptop computers

Medical Devices

ECG equipment
TPN Compounding equipment
Ultrasound machines
Audiology and systems spectrometry equipment
Autoclaves
Infusion Pumps
Intensive Care Unit equipment

Communications and Networking

Network equipment
Telephone switchboards
Pagers/mobile phones
Telephone Switches and PBX

Building and Office Systems

Plant/Boiler Management
Energy management Systems
Light Controls
Alarms/Security Systems (fire, intruder, security, environment monitoring)
Automatic Doors, Vaults, and Gates
Access Control Systems
Video Monitoring Equipment
Office Equipment: Photocopiers, Fax Machines
Elevators/Escalators
Heat/Ventilation

In general, existing site-specific equipment lists (if any) are neither exhaustive nor do they readily identify why or if a certain equipment type is prone to Year 2000 problems. The remainder of this section provides some information on how to decide if a system or equipment item could have a Year 2000 problem.

2.4 Characteristics Of The Problem

There are certain functional and constructional characteristics that can identify a computer system or item of equipment as potentially at risk of failure because of a Year 2000 problem. The presence of these characteristics does not imply that the equipment will exhibit problems but rather identifies that the system or equipment should be subjected to further detailed analysis.

Some of the functional characteristics that offer an indication of potential failure are summarized below:

- displays a date or time
- requires entry of date and time on start-up
- implements a timed control sequence
- performs operations on a timed basis
- produces hourly/daily/weekly/monthly reports
- calculates any time-based totals, averages, rates, or trends
- time stamps data, or uses time stamped data
- maintains historical data
- handles timed alarms and events
- generates alerts at pre-determined times (e.g., planned maintenance or calibration)
- has rolling database files (i.e., delete oldest entry when new one added)
- requires accurate calibration on a predetermined schedule for operation

There are also a number of constructional characteristics that help identify potential problem systems and equipment. However, these are less easy to determine by non-technically oriented personnel. Some of the more obviously visible of these characteristics are:

- communicates with other computer systems
- uses specially written software (e.g., "middleware")
- PC (personal computer) based

PC-based systems have received a significant amount of coverage in the media and are candidates for further investigation wherever they are in use. The PC Date Rollover (i.e., the transition from 31st December 1999 to 1st January 2000) may have to be tested locally by the health care provider site if the supplier/manufacture is unable or unwilling to verify the Year 2000 compliance of the system.

IMPORTANT: Whenever any testing has to be undertaken locally, it should be planned and carried out with great care and due regard to the consequences of failure of the equipment under test. It is highly recommended that the vendor or supplier of the equipment or system be contacted for appropriate test strategies. A request for the vendor to be present for the tests is also a prudent measure.

EVEN MORE IMPORTANT: Any on-line testing must be carried out with great care, and with an acceptance by all of the potential consequences of test failure. **ENSURE THAT THE BACKUP/RECOVERY PROCESS IS IN ORDER!** Test the backup/recovery process first if you must to be SURE it works before subjecting the system to Year 2000 testing. It is not unknown for automatic tidy-up routines to delete 'old' data after moving the date forward and wipe out the entire historical storage of patient records, of dispensing records, of business records, of ...whatever!

OF GREAT CONCERN: Be very careful if you do the testing yourself and make sure you do not test a live system. Resetting the computer's clock can play havoc with the system and may actually cause the very problem you are trying to avoid. It may be worthwhile to employ a specialist contractor or consultant to assist you.

2.5 Linked Systems

Most systems do not operate in isolation. We need to include the possibility that inputs to the system being considered (e.g., from another system or equipment item) are erroneous or missing because of Year 2000 problems.

We also need to consider the outputs from the system being assessed. If there is a possibility that the outputs are incorrect because of a Year 2000 problem, will this affect another system, which in turn may have an impact on safe and continued operation or on safe and continued patient care?

3. AN APPROACH TO SOLVING THE PROBLEM

The Year 2000 problem has been described. The chaos that could result from non-compliant Year 2000 systems and equipment has been described. Now, what is a health care provider to do? Start resolving your Year 2000 problems now so that they are not a problem when the new century arrives!

This section presents a five-step approach to tackling the Year 2000 problem in any health care provider site:

- Awareness
- Inventory/Audit
- Analysis
- Remediation/Action
- Clean Management of New Systems

These steps are described in more detail in subsequent sections.

3.1 Awareness

Year 2000 Awareness is “making sure everybody in the health care provider site is aware of the problems that might occur”. This awareness raising has yet to be fully addressed and is the subject of on-going planning within government and industry. Until greater awareness has been achieved, it may remain difficult to determine the full range of equipment and systems affected by the Year 2000 problem.

The extent of the Year 2000 problem and the different systems and equipment that can exhibit the problem are initially addressed in Section 2, *Nature Of The Problem*. These are not exhaustive lists, but highlight the wide-ranging extent of the systems and equipment that must be reviewed within a pharmacy or other health care provider site.

3.2 Inventory/Audit

The title for this step has been presented as both Inventory and as Audit. The primary intent of this step is to identify all computers, computer software, and other equipment or systems that use computer-based, or embedded, processing. To achieve this, an inspection of **all** equipment, medical and non-medical, has to be carried out and an inventory drawn up. This inventory is a list of all systems and equipment that you have at your health care provider site that could possibly be affected by Year 2000 non-compliance.

In generating the inventory, it may be helpful to review Section 2.2 above that contains a list of potentially vulnerable systems and equipment items. As part of the inventory process, determine if an external maintenance provider maintains the system or equipment item, and whether you have a copy of the maintenance contract. This could be useful if you have a dispute with your supplier about costs of upgrades. Remember that problems are already occurring with some systems because they deal with dates in the future.

The identification of PCs and PC-related software should be a relatively straightforward task.

The identification of equipment items with embedded processing may require consideration of the functional and constructional characteristics of the equipment. Section 2.3 above describes these functional and constructional characteristics that aid in the identification of embedded processor equipment.

There may be some equipment that is not readily identifiable as processor based. These may require external assistance, preferably from the vendor, to evaluate or require the equipment to be opened-up for a more detailed inspection. The opening-up of equipment has associated problems and risks, and should only be considered as a last resort.

If in doubt, add the equipment item or system to the inventory and resolve the issue later.

Section 4.0 below describes Inventory/Audit in greater detail.

3.3 Analysis

The inventory/audit forms the basis for the Analysis step. Each inventory item and system needs to be checked to determine if it might suffer from Year 2000 problems. This will include most PCs: manufacturers estimate that 80% of PCs will fail to handle the Year 2000 properly.

A number of Year 2000 guidance documents outline that you should ask your supplier, or whoever supports your system, for information first, but it is *advisable* to get written evidence of compliance. It is strongly recommended that written evidence of compliance be obtained and that the responses are checked for accuracy and completeness.

A full set of compliant and unambiguous supplier/manufacturer responses may not be readily available. Therefore, you must assess the impact of failure (i.e., Impact Analysis) for each piece of equipment and system. If the supplier of the system/equipment is no longer in business, or if you have written the system yourself (in-house), you may have to test it yourself. Be very careful when you do this and make sure you do not test a live system. Resetting the computer's clock can play havoc with the system and may actually cause the very problem you are trying to avoid. It may be worthwhile to employ a specialist contractor or consultant to assist you

As part of an Impact Analysis, each of the systems and equipment items should be prioritized for Y2K issue resolution. This will help to ensure that the best use is made of available resources. The results of Impact Analysis, together with the supplier/manufacturer responses, will help identify what subsequent steps have to be taken for each system and equipment item, and the relevant priorities for resolving the Year 2000 issues.

See Section 5 below for more information regarding the Analysis step.

3.4 Remediation/Action

The Inventory/Audit and Analysis steps generate a comprehensive inventory and a Year 2000 compliance status for each piece of equipment. Normally, the higher priority systems and equipment should be addressed first and plans should be drawn up for each of the non-compliant systems and equipment to:

- Replace with a compliant alternative
- Live with it
- Upgrade in conjunction with the original supplier
- Add a work-around
- Revert to manual operation.

See Section 6.0 below for details of the Remediation /Action step.

3.5 Clean Management Of New Systems

In parallel with the handling of existing systems and equipment items as outlined above, you need to ensure that the procurement of new equipment, or replacement of non-compliant equipment, is free from Year 2000 problems. Be aware that systems and equipment being purchased off the shelf today most likely contain Year 2000 problems.

There are a number of ways of minimizing this risk, including suitable clauses in the acquisition contract or additional Year 2000 tests as part of the acceptance process.

4. INVENTORY/AUDIT

The primary intent of this step is to identify all computers, computer software, and other equipment that use computer based, or embedded, processing. To achieve this, an inspection has to be carried out on **all** equipment and systems and an inventory drawn up.

4.1 Inventory

The inventory is a key document and any errors or omissions at this stage may go undetected for some time. The identification and inclusion of the embedded processor equipment is the area where most omissions arise. It is also the area that is most difficult for non-technically oriented personnel to resolve. Several large commercial organizations have overlooked embedded processors in their original inventories and have been forced to re-work their inventory and revise their project and resource plans.

The identification of individual PCs and PC related software should be a relatively straightforward task. What is more demanding for these systems and software is the identification of version numbers and serial numbers which will be required, on many occasions, by the suppliers and manufacturers to aid them in uniquely identifying equipment in use.

When a whole PC based system has been procured from one supplier, that supplier should be the sole contact for a comprehensive response. However, a number of hardware items may have been added to the system following the original procurement (e.g., fax-modem or other communications card). When this is the case, the suppliers of these add-ons must be contacted for a compliance statement. Again, version number and serial number will be important.

All software packages resident on a PC will need to be identified and included in the inventory. Software packages must be recorded for at least two reasons. First, the package may be manipulating time and date as one of its normal functions and therefore must be assessed for Year 2000 compliance. Second, the package may read the time and date from the PC clock mechanism for display purposes and should the clock mechanism fail, then the package may also act erroneously.

In addition to the more visible application level packages, which perform some obvious function for the user, it will also be necessary to include the operating system related software in the inventory.

The identification of equipment with embedded processors is not always simple or obvious. To facilitate their identification, consider the functional and constructional characteristics of the equipment (see Section 2 - *Nature Of The Problem*).

If in doubt, add the equipment or system to the inventory and resolve the issue later.

There will be a number of pieces of equipment that are not readily identifiable as processor based. These may require external assistance, preferably from the vendor or original equipment manufacturer (OEM), to evaluate or require the equipment to be opened-up for a more detailed inspection. The opening-up of equipment has associated problems and risks and should only be considered as a last resort.

The inventory entry for each equipment item should contain, as a minimum:

- Name of equipment/software/system, etc.;
- Model number;
- Function;
- Addresses and contacts for suppliers, manufacturer, and maintainers;
- Version number;
- Serial number;
- Support/warranty position;
- Location of the system/equipment item at the health care provider site.

4.2 Related Documentation

4.2.1 User Manuals

Most of the items in the inventory can be identified as potentially having a Year 2000 problem by visual inspection. Reference to existing asset lists and maintenance schedules can provide supporting input to the inventory but it should be remembered that such documents might not be current. Supplier documentation in the form of User Guides and Maintenance Manuals can also be useful sources of information to confirm the existence of a real time clock or time based functionality.

4.2.2 Maintenance And Warranty

Contract documents and maintenance agreements can also help identify the existence of supplier support and warranty agreements that make a commitment to rectify and/or replace any Year 2000 defective equipment. Support and warranty agreements are rarely for the full life of the equipment supplied so it is worth checking at least the coverage offered by the contract and whether it needs renewal prior to Year 2000.

NOTE: The absence of a support and warranty contract may not mean that your supplier is not under an obligation to support your Year 2000 problems. This is currently an area of contention. Advice in this respect may be required from a member of the legal profession.

5. ANALYSIS

5.1 Supplier Contact

The Inventory/Audit step and the inventory list produced from it form the basis of the Analysis step. Each inventory item should be checked for Year 2000 Compliance with the supplier.

Supplier Contact aims to determine whether the supplier believes an equipment item or system is compliant. It does not determine absolutely the compliance status of an equipment item or system, because there is the possibility that an equipment item or system claimed by a supplier to be compliant will prove to be non-compliant. However, supplier contact does provide useful information and is an important exercise.

Experience shows that to get the best possible quality of response, it is important to:

- **Prioritize your equipment/systems** – Because of the potentially large volume of equipment and systems, it is obviously best to prioritize your equipment/systems based on criticality and then focus your vendor management efforts on the most critical items first. A recommended prioritization scheme for Y2K problem resolution is based on the effect of failure on Life, Health, Safety; Safeguarding Resources (inventory, facility, payroll, receivables); Mission Critical; High Visibility (public outcry); and Other.
- **Be specific** - Give as much specific detail as possible as to the make and model, and its use. This will help the supplier narrow the area to be investigated;
- **Be persistent** - As the Year 2000 approaches, suppliers will be extremely busy;
- **Do not threaten** - This will not encourage cooperation, only legal wrangles; stress that this is a request for cooperation;
- **Keep records** - Record all correspondence and contact, both written or verbal;
- **Anticipate delays in receiving responses** - Delays will grow as more companies realize their responsibilities and exposure, and seek information from suppliers/manufacturers.

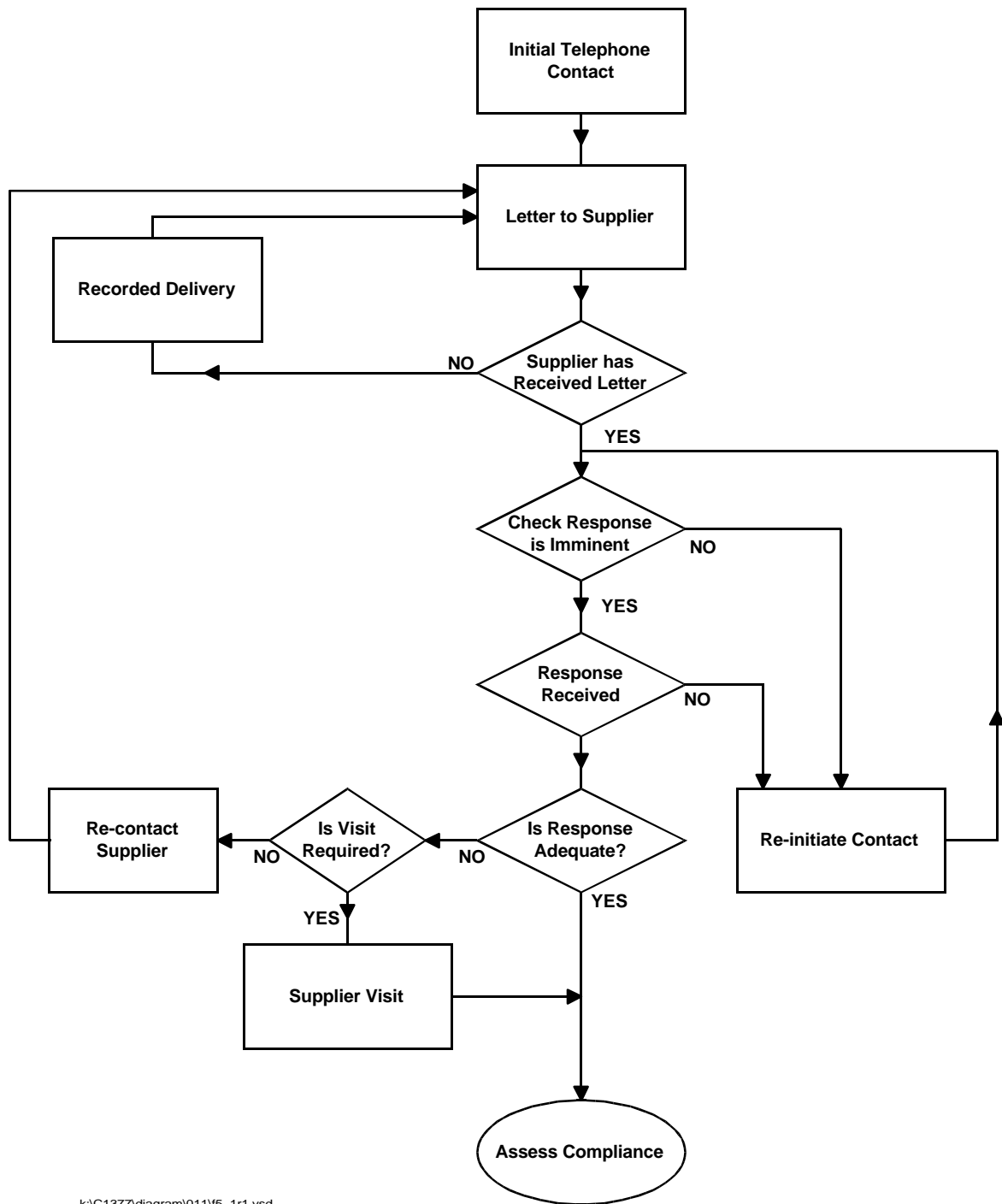
Figure 5.1 (see Page 15) contains a flowchart describing the sequence of activities associated with supplier contact. These activities are as follows:

- **Initial telephone contact** - Call the supplier to determine if the supplier has nominated an individual within its organization to deal specifically with Year 2000 issues relating to its products. Call the nominated person and make them aware that you are dealing with the issue for your organization. If the supplier no longer exists, see below (unsupported software).
- **Letter to supplier** - Send a letter to the nominated person in the supplier organization requesting details of compliance. If there is not a nominated person in the supplier organization, address the letter to a senior employee. The letter should also give a target response timeline (2 weeks is not unreasonable).

- **Verify supplier has received letter** - Contact the supplier to verify that it has received the letter. If it has not, re-mail the letter, and use registered/signature required delivery. If the supplier has received the letter, confirm that it will be able to respond within the required timeline, and if it cannot, agree to a revised timeline.
- **Verify supplier response is imminent** - Between 3 days and a week before the response from the supplier is due, contact the supplier to check that it plans to respond within the required timeline.
- **Review the response** - When the response from the supplier has been received, check to ensure that it is a complete response, and that it has not omitted any key issues. If any issues are not successfully addressed, re-initiate contact with the supplier. Assessing supplier responses is dealt with in more detail later in this section.
- **Supplier Visit** - If it seems apparent that the supplier is having difficulty responding, or if testing is perceived to be necessary, request a supplier visit to assess compliance.

5.1.1 Unsupported Software or Equipment

There may be equipment and software in use which are no longer supported by a supplier or by the original manufacturer. The method for dealing with these cases will probably depend on the amount of information available, and how difficult it will be to replace the item. If it is a software package and there is a definite Year 2000 problem, it may be possible to fix it. If the source code is not available, the options are reduced. When the item in question is a piece of equipment with an embedded system, it may or may not be possible to determine whether it is Year 2000 compliant. If it is not possible to determine compliance, the impact analysis will dictate whether or not the piece of equipment must be replaced.



k:\C1377\diagram\011\6_1r1.vsd

Figure 5.1 – Supplier Contact

5.2 Assessing Supplier Responses

When a supplier has asserted compliance, it is essential to verify this. Asking whether the supplier can demonstrate compliance and, where appropriate, viewing that demonstration, can differentiate between those suppliers who think that they are compliant, and those who know that they are. However, it may be difficult to set up a test environment that will allow a full test of how an application will work over the century change and beyond.

For those equipment items that are not compliant, it is important to quickly determine when a compliant version will be available, how much it will cost, and what other changes may have to take place in order to achieve compliance.

What happens if the supplier does not reply to inquiries, and how much trust can be placed in the reply if you do get one? The answer in both cases will depend on the priority of the equipment item or system. The higher the priority of the equipment item or system, the more effort should be spent talking to the supplier and testing in-house. Some in-house testing will be essential, as it is unlikely that the supplier will have been testing the equipment item or system using exactly the same configuration of software or hardware as that which exists at the health care provider site.

Similarly, when the equipment item is not compliant and the supplier plans to produce a compliant version by a date that is too far in the future, it may be better to find alternatives and plan contingency early on (given that many projects fail to meet time deadlines!).

5.3 Impact Analysis

Impact Analysis, the impact of failure, must also be assessed for each system and equipment item in the inventory. The result of this activity together with the supplier/manufacturer responses will help identify what subsequent steps have to be taken for each system and equipment item and in what order each Y2K problem should be addressed.

As part of the Impact Analysis, each system and equipment item should be prioritized to ensure that the best use is made of available resources. The prioritization should be based on what the effect of failure of the system or equipment item would be. One such prioritization scheme is as follows:

- **Priority 1 - Life, Health, Safety Threatening:** determine if patients' lives, employees' lives or the viability of the organization could be at risk;
- **Priority 2 - Critical or Safeguarding Resources & Assets:** determine if it would be very difficult to treat patients or for the organization to function at all;
- **Priority 3 - Important:** determine if it would be difficult to continue as normal; this includes the High Visibility problems that would present themselves in the public eye or media and pose a considerable barrier to continuing effective work;
- **Priority 4 - Manageable:** determine if there would be problems but these could be overcome;
- **Priority 5 - Minimal:** determine if the effect would be insignificant.

5.4 Testing

A full set of compliant and unambiguous supplier/m manufacturer responses is unlikely to be readily available. When sufficient supplier information is not available, some testing may have to be carried out locally to support or augment supplier statements.

Bearing in mind the fixed timeline for successful project completion, do not misapply expertise. It is too valuable. To this end, decisions should be made on which equipment items and systems should be subjected to testing:

- If the equipment item or system is going to fail totally do not waste effort on it. Initiate the repair or replacement program.
- Concentrate on the high priority equipment items and systems where there is little supplier support information or where there are doubts or ambiguities in the supplier responses.
- If you are certain you can survive the nature of the failure and the priority of the equipment or system is low, **document your acceptance of the problem** and schedule the repair or replacement for a later time once higher priority items are dealt with.

Testing needs to be considered with care, since it carries with it a likelihood of failure. Some considerations before carrying out testing are as follows:

- Assess the consequences of the equipment item or system failing or behaving improperly as a result of testing.
- Supplier demonstrations of compliance are preferred, but only if they use a representative equipment item or system.
- **Off-line** is preferable, but be prepared for consequential effects when you re-introduce the equipment item or system into service.
- **On-line** testing should be carried out with great care and with an acceptance by all of the potential consequences of failure.
- Ensure that the Backup/Recovery process is in order. It is not unknown for automatic tidy-up routines to delete 'old' data after moving the date forward and wipe out the entire historical storage.
- Ensure that **at worst** the equipment item or system can be re-initialized to a different state (e.g., all storage blanked, all formats at default levels).
- Use a spare equipment item or system if possible and if identical.
- **Document the test process and the results.** It may be necessary to repeat, or to step back through the process to determine when a fault/error actually occurred. The documentation may also be helpful should you be unfortunate enough to be involved in any litigation surrounding the Year 2000.

Testing is not a simple case of setting the date and time to 31 December 1999 and waiting to see what happens when the year changes. AGAIN, DO NOT DO THIS ON LIVE EQUIPMENT OR SYSTEMS WITHOUT PROPER BACKUP AND PLANNING.

There are a number of dates that can potentially cause failure. Similarly, there are a number of functions that are most likely to cause failure. These include:

- rollover (power on and power off check across both the century change and leap year transitions);
- trigger dates (generally at the whim of the programmers, e.g., 1/1/1, 9/9/99, 1/1/99);
- date ranges (software that survives rollover often cannot provide data over a range that spans the year change or even the leap year day);
- utilities (sorting, purging, tidy-up and history handling software can be problematic, especially in database systems).

Systems and equipment items rarely operate in isolation. There is generally an interface or data exchange between various systems and equipment items. Should an equipment item or a system fail a test, the impact this will have on the other equipment items and systems with which it communicates needs to be considered.

5.5 Inventory And Analysis Report

Having identified all of the equipment items and systems and their Year 2000 compliance via a mixture of supplier responses and testing, you are now in a position to consider the technical solutions for each equipment item or system that is known to fail.

Each technical solution should be documented together with:

- the impact of the solution on safety;
- the timelines for implementing the solution;
- the cost of implementing the solution;
- the ease (or difficulty) of implementing the solution;
- the acceptance criteria for the solution (noting that a partial fix may be acceptable for some equipment items or systems); and
- a Contingency Plan in the event the solution is not viable or the timeline for the solution is not acceptable.

5.6 External Assistance

The Inventory/Audit and Analysis steps described have assumed that the health care provider itself will carry out all of the related activities. This assumption is consistent with the understanding that the provider itself is responsible for resolving the Year 2000 problem within the health care provider's business.

A significant number of equipment items and systems are going to be common across various health care provider sites throughout the country. This will lead to obvious replication of effort across provider sites and also by suppliers in responding to inquiries.

Currently there is no central facility or formal procedure in place to minimize this inefficiency. However, several federal agencies and industry trade organizations worldwide are currently maintaining a set of WEB pages detailing manufacturer responses for a variety of commonly used medical devices. These can be found by searching the Web using "biomedical" and "Y2K" as search arguments.

6. REMEDIATION/ACTION

The Inventory/Audit and Analysis steps should generate a comprehensive inventory and a Year 2000 compliance status for each system and equipment item. The higher priority systems/equipment should be the focus of remediation action and addressed first. Plans should then be drawn up for each of the remaining non-compliant systems and equipment.

The time available to deal with a Year 2000 problem is becoming very short. At this point there is insufficient time for making decisions by consensus among many individuals. To this end the overall strategy should be implemented and managed by an individual with sufficient authority to ensure that all necessary tasks are expedited and completed.

The **main strategies that may be adopted to minimize the Year 2000 problem** include:

- replace it
- ignore it – accept risk
- fix it
- work-around it
- revert to manual operation.

Additional considerations to address before choosing the appropriate strategy for each system or equipment item are detailed in the following paragraphs.

In adopting any of these strategies, it will be necessary to reassess compliance by generating acceptance criteria and, in many cases, re-testing the replacement, or refurbished, equipment item or system. This is essential not only to ensure that the failure is no longer present, but also to ensure that no additional failures (not necessarily date related) have been introduced.

6.1 Replace It

On the face of it, this is the simplest solution. If a system or an equipment item will suffer from a potential failure - replace it. However, in reality a number of other factors come into play, for example:

- Is the replacement system or equipment item Year 2000 compliant?
- Is the replacement's functionality identical to the original? If not, what is its impact on interacting systems/equipment and the overall operation of the system/equipment item?
- Have all issues relating to safe and continued operation been adequately addressed?
- Are adequate funds available to support procurement?
- Are adequate resources available to support acceptance testing and commissioning?
- Can you get the replacement system implemented and up and running in your environment prior to the failure of the old system?

6.2 Ignore It – Accept Risk

It may be practical to ignore some potential failures on the basis that safe and continued operation is not compromised. However, consideration should be given to the following:

- Is the expected failure adequately documented so as not to cause unexpected reactions on the part of the operators/users of the system/equipment item?
- Will any other system/equipment item react inappropriately because of the failure?
- Have the results of the failure been fully justified to any necessary authorities and deemed acceptable (e.g., wrong date on a patient record, or wrong quality control date on a maintenance certificate, etc.)?

6.3 Fix It

If a 'Fix' does not result in a complete return to the previous performance, functionality and characteristics of the original equipment item or system, it should be regarded as a replacement and treated accordingly.

Any change to software code, configuration data or logic code should be regarded as an upgrade and require re-acceptance.

Testing of any fixes should be complete and inclusive. ALL original functionality, as well as Y2K compliance, should be tested on any system or equipment item which has been 'fixed'.

6.4 Work-around It

A work-around can be purely procedural (e.g., manually change the date on all outputs, or restart the system/equipment item every morning) or may involve additional processing of inputs and outputs to the system/equipment item. In the latter case, this should be regarded as a replacement system/equipment item and treated accordingly.

If additional operations are required to achieve the work-around, their impact on safety should be assessed and appropriate staff trained to accomplish the work-around.

6.5 Revert to Manual Operation

Any reversion to manual operation is subject to a number of considerations:

- What is the impact of prolonged manual operation?
- Are additional procedures or equipment required?
- When was manual operation last utilized?
- Are there sufficient numbers of competent staff available?

6.6 Contingency Planning

The best made plans can go astray. Projects associated with computers and software are notoriously difficult to bring in on time, and a Year 2000 project will be no exception. Any proposed Year 2000 project timeline is additionally risky because it is exceptionally difficult to assess the manpower required to accomplish it and industry staff shortages may make it very difficult to secure the numbers of technically skilled staff needed to ensure a timely project.

For these reasons, contingency plans need to be drawn up in parallel with the main plans, or as quickly as possible thereafter. **Contingency plans should consider methods by which the health care provider can guarantee continuity of service if the remediation program fails (for whatever reason).**

Alternatively, if a system or an equipment item is known to be at risk, and the planned fix is running late, a temporary solution may have to be introduced. At what point in the schedule does the decision need to be made to specify and purchase the additional system/equipment?

Contingency plans should, of course, be continuously revisited and updated as the project proceeds in order to guard against the worst-case scenario of being unable to guarantee safe and continued operation across a range of services in the Year 2000.

6.7 Ownership Considerations

The assets and infrastructure of health care providers vary widely. A large health care provider may own all of the systems and equipment in the business as well as owning the building itself and thus also be responsible for building services, security, etc.

The previous sections in this report assume that the building and the systems and equipment within the building are owned by the health care provider. If this is not the case, the information previously outlined is still valid but consideration needs to be given to at least three additional factors:

- Building ownership and the extent of the services supplied by the owner;
- Leased ownership and the extent of the services supplied by the lessor (e.g., switchboard, facilities, HVAC);
- Health care provider corporate/business ownership.

These additional factors require agreement by the parties concerned as to who is responsible for each system and equipment item. Depending on when this is done, it may be necessary to compare inventories to ensure that no equipment item or system is overlooked. From the health care provider viewpoint, the other parties should be considered thereafter as normal suppliers and, as far as possible, dealt with accordingly.

Because of the close relationship and dependency between the parties sharing a multi-ownership site, it may be necessary when reviewing action plans, etc., to ensure that the other parties are not significantly affected by any change in your priorities. Similarly, if the other parties change their priorities it may be essential that you are aware of these revisions.

6.8 Supply Chain Considerations

All health care provider sites rely on suppliers of goods and services to varying degrees, including the actual equipment and other items owned/used within the business, typically in line with the following:

- utilities (electricity, water, gas, phone);
- wholesalers (e.g., drug supplies, medical gases, medical devices);
- service providers (e.g., medical equipment calibration/certification, maintenance, federal express/airborne/ups).
- Specialty products (e.g., radio-pharmaceuticals, blood products, etc.)

These service and product suppliers are normally critical to the operation of the health care provider and in many cases may be required by federal and state legislation to operate.

These suppliers/service providers should be treated as normal suppliers and treated accordingly, including contingency planning if they should fail to meet their responsibilities due to their own unresolved Y2K issues.

APPENDIX A

THE INDEPENDENT Rx PHARMACY

A.1 Introduction

This appendix presents the findings of a Year 2000 analysis of a typical independent retail pharmacy called "The Independent Rx".

This appendix also identifies some of the characteristics that help identify why a particular piece of equipment or system at *The Independent Rx* pharmacy may potentially have Year 2000 related problems. These characteristics may exhibit themselves in similar equipment at other health care provider sites.

A.2 Scope

The scope of the general Y2K Review is:

"To review the operations of a typical retail pharmacy to provide suggestions to the pharmacy management to:

- Determine current Y2K plans and activities;
- Help identify equipment and systems that may be affected;
- Help determine required action to investigate identified equipment and systems;
- Establish possible extent of the problem in that pharmacy and extrapolate across all pharmacies and health care provider sites in Ohio; and
- Produce information and suggestions which can be disseminated and applied to all State of Ohio health care provider sites."

A.3 Determine Current Y2K Plans And Activities

Current Y2K plans and activities of this health care provider site are presented using a Five Step Approach:

- Awareness
- Inventory/Audit
- Analysis
- Remediation/Action
- Clean Management/New systems.

A.3.1 Awareness

Mr. Frank Proprietor (Senior Pharmacist) is well aware of the Year 2000 problem and its potential consequences. Most of R.Ph. Proprietor's understanding is derived from his personal knowledge of PCs and his positive attitude towards technology. He is also a standing member in the Columbus Year 2000 Users Group, which, along with recent articles in professional journals, has raised his awareness. This level of awareness is not considered representative of pharmacy owners in general.

A.3.2 Inventory/Audit

No formal audit activities have been documented. An asset register used for insurance and accounting purposes is in place. This may provide a reasonable starting point for creating an inventory for the pharmacy systems and equipment. Caution must be employed, as this will almost certainly not contain all potentially affected equipment and systems. The identification of model numbers, serial numbers, and software version numbers could be a more demanding task.

A.3.3 Analysis

Although no analysis had been initiated by the pharmacy, they have received correspondence from a couple of suppliers, one of which had indicated that two of the software products they supplied are non-compliant. One of the packages has subsequently been upgraded, with the other due to be upgraded at the end of the financial year. The other supplier has replaced the relevant hardware.

No other analysis related activities have been carried out.

A.3.4 Remediation/Action

A prioritized remediation or action plan is based primarily on the outcome of the previous steps. With little formal progress to date in these activities, it is too early to expect a plan to be in place.

A prioritized action plan should be drawn up at the earliest opportunity to ensure, at least, that the main steps are identified and understood. As the main steps progress, this plan should be revised to ensure that the remaining activities are prioritized to make optimum use of the limited resources available to address the equipment items and systems at risk from the Year 2000 problem.

A.3.5 Clean Management/New Systems

R.Ph. Proprietor recognizes that new equipment and software will be required between now and the end of the century. Like many independent retail pharmacies, his pharmacy does not have the capital resources available to fund all of the required changes. R.Ph. Proprietor will need to address this as soon as possible.

Some pharmacies may be a single entity in a chain from a much larger corporation. The pharmacy manager may have limited assurances from his corporate entity that Y2K fixes and new Y2K compliant systems are "forthcoming". Yet, even under this corporate umbrella, the pharmacy manager is responsible for the purchase of all equipment and systems used by his pharmacy. It is anticipated that if the appropriate corporate procurement guidelines are followed should any new equipment or system be procured, then minimal disruption should arise from these replacement systems.

A.4 Help Identify Equipment/Systems That Might Be Affected

A.4.1 Inventory/Audit

The identification of equipment and systems that potentially could suffer from a Year 2000 related problem requires an Inventory and Audit to be carried out to identify **all** computers, software packages that reside on these computers, and computerized equipment using embedded processors.

The identification of computerized equipment, which utilizes embedded processors, is not a simplistic task for the non-technically oriented. However, there are systems and equipment lists available (see Section 2 - *Nature Of The Problem*) that identify a number of such systems.

The following 'equipment/systems' were identified or discussed during the analysis as being used by *The Independent Rx* pharmacy:

- Dispensing standalone PC – running DOS and Windows
- Business administration software package
- Backup standalone PC - running DOS and Windows
- Payroll and Accounts software packages
- Fax Machine
- Telephone system
- Electronic Delivery & Tracking (EDT) system
- Intruder alarm
- CCTV
- Electronic cash register
- Electronic Tag system.

Other areas discussed but that were not part of this pharmacy's equipment or systems were:

- Electronic tablet counters/Automated Dispensing systems
- Electronic scale
- Autoclave
- Fire system

The main risk areas as far as this pharmacy was concerned were:

- Dispensing standalone PC
- Business administration software package
- EDT
- Payroll and Accounts software packages
- Intruder alarm

A.4.2 Analysis

Having carried out an audit and identified the computerized systems and equipment, the suppliers should be contacted for written evidence of compliance for the equipment or systems of their supply. Supplier responses will vary in quality and many will not fully resolve the issue of compliance.

The identification of supplier responses that do not address the relevant issues requires an understanding of, at least, both the structure and functionality of the equipment and systems under analysis. The amount of effort that should be expended on following up these supplier responses depends very much on the impact that the equipment has on the business. Equipment that displays or utilizes the date should, at least, solicit an explicit response from the supplier that the equipment has been subjected to testing and the result(s) of their testing.

A.4.3 Potential Problems With Equipment/Systems At *The Independent Rx Pharmacy*

Dispensing standalone PC – Running DOS, Windows and MSWorks

The business administration software package on this PC performs maintenance of patient records, drug interaction checks, generation of prescription labels, generation of reports/data required by state and federal law, ordering from wholesalers, etc. Many of these functions are date dependent. The supplier has indicated that this package "will not be supported beyond 1999".

Does this imply that the software package is not Year 2000 compliant?

The compliance status of the software should be clarified with the supplier, with upgrade options available should the package be non-compliant.

The usage of date functionality within software packages is not always evident. Therefore, all software packages running on PCs should be checked with suppliers as to Year 2000 compliance.

A possible implication of upgrading software is that the new upgraded package may not run on the old PC hardware platform, therefore necessitating the upgrade of the hardware also, adding to the overall cost and complexity of resolving the Y2K issues.

PCs are the one area where a significant number of failures will occur. Manufacturers estimate that up to 80% of currently installed PCs will fail to handle Year 2000 properly. In this case, the standalone dispensing PC is a 486 SX25 based system, with a high probability of failure.

Be aware that not all versions of Unix, DOS or Windows operating systems are Year 2000 compliant.

Backup standalone PC

This PC is used as a backup to the dispensing PC during maintenance, software upgrades, etc. The system is a 286 based PC and as such is highly likely to fail. This equipment need not be checked with the supplier as failure is expected and replacement is much easier than repair. Similarly, the operating system and any other application packages used on the PC should be checked.

Fax Machine

The fax machine is of an older generation and does not appear to have any time/date functionality. A visual inspection of the machine and a review of the operating manuals determined this. No further action is required in this case.

Electronic Delivery and Tracking (EDT)

This system is used to order supplies from one of the two wholesalers used by the pharmacy. The PIP (Pharmaceutical Interface Product) code is entered as a seven-digit number along with the quantity required before being transmitted to the supplier. There is time and/or date functionality on the display. This equipment is crucial to the operation of the pharmacy, therefore the manufacturer should be contacted and further investigations initiated.

Intruder Alarm

This system displays the time and date on the front of the control panel. The supplier has recently upgraded the system. This upgrade is believed to be Year 2000 compliant. However, no formal Year 2000 tests were conducted on the system, therefore the supplier should be contacted for written compliance and/or test results.

CCTV

This system is composed of a digital multiplexer, cameras, monitors and a video recorder. The monitors display time and date. It should also be noted that in some CCTV systems the cameras also have independent time and date functionality. The supplier should be contacted regarding all the equipment.

Electronic Cash Register

The date is printed out on customer receipts. This equipment should be checked with the supplier.

In some pharmacies, this system may be connected to an EPOS (Electronic Point Of Sale) system, which would require further investigation and contact with the supplier as it will may have inherent time and date functionality.

Electronic Tag System

This is a PC based system comprised of a 486-based PC, magnetic detector, display, operating system software and application software.

The system has the ability to record events, which can be downloaded for review by a service engineer. These events and files in the system are likely to be date dependent. This system should be referred to the supplier.

The following items were discussed, but were not part of the equipment at this particular pharmacy:

Electronic Tablet Counter/Automated Dispensing System

This equipment can be microprocessor based and as such should be checked with the supplier.

Electronic Scale

This equipment can be microprocessor based and as such should be checked with the supplier.

Autoclaves

There is a time cycle associated with most autoclaves. Some autoclaves have been deemed to be non-compliant; therefore this equipment should be referred to the supplier.

A.5 Help Determine Required Action To Investigate Identified Equipment

The investigation actions should be addressed in two phases. The first of these two phases is to identify who actually owns the problem. Once this is established, the next phase is to determine the extent of the problem and the action to be taken in resolving the problem.

Ownership of the problem will vary from pharmacy to pharmacy and is dependent on at least three factors:

- Building ownership and the extent of the services supplied by the owner;
- Leased ownership and the extent of the services supplied by the Lessor (e.g., telephone switchboard);
- Pharmacy business ownership.

A further phase may be required to compare and revise action plans developed by the different owners of the problem. This phase will help to ensure that the level of risk and action plan developed, say by the Lessor, takes full cognizance of the requirement of the end user (the pharmacy).

A.6 Establish Possible Extent Of The Problem In This Pharmacy And Extrapolate Across All Pharmacies In Ohio

The extent of the problem within this pharmacy is considered initially with respect to the main risk areas identified above.

The business administration software package forms the core system for pharmacy business administration, including maintaining patient histories, performing drug interaction checks, generating prescription labels and drug information sheets, generating reports required by state and federal laws, ordering stock, etc. The software package is believed to be in use in a significant number of pharmacies, with other pharmacies using similar packages from various suppliers.

The EDT system is also believed to be in use in a significant number (if not all) of the pharmacy sites in Ohio. These types of systems are likely to differ in model and supplier from pharmacy to pharmacy.

The payroll and accounts packages are fundamental to the running of the business.

With all of the above, there are likely to be multiple suppliers and packages which, due to the limited technical knowledge and skill level of the end users, are potentially concerning unless there is a Pharmacy User Group that is addressing the variety of packages on behalf of the various practices.

A.7 Produce Information And Suggestions Which Can Be Disseminated And Applied To All Ohio Pharmacies

This appendix has been developed for pharmacies to provide initial information and suggestions on tackling the Year 2000 problem and to identify key activities to be carried out in conducting a Year 2000 rectification program.

This appendix also gives some examples of why a particular piece of equipment has the potential to disrupt a pharmacy practice site, and the functional characteristics of a piece of equipment make it a candidate for further consideration.

<><><>