Y2k 18249 – college essay

This year, most of the world is preparing to celebrate the year 2000 and the coming of a

new millennium. However, many businesses, manufacturers, banks and hospitals are

quietly hoping for an uneventful new year's transition. At midnight on December 31,

many businesses will be anticipating what effects the millennium rollover will have on

computer software and other equipment that contain a time sensitive chip called an

embedded chip. Early computer programmers, in an effort to conserve limited memory

space, programmed computers to read the year in only two digits. So computers read 15

as 1915, and 02 as 1902, and so on. Thus, when the year 2000 arrives, many computer

programs might go from December 31, 1999 to January 1, 1900. Some computers will

cease to function, or " crash". Needless to say, if these programs control functions such as

electricity, airline travel, or communications, the results could be disastrous. Many

companies and governments have spent countless hours and untold dollars making

software Y2K (year 2 thousand) compatible.

The consequences of not preparing for the Y2K problem could spell disaster for

the company involved. For example, a small Midwestern manufacturer encountered a

similar date-related problem in 1996 (a leap year) when the company did not realize that

their entire computer network would be affected by the extra day in the year. When the

year 1997 turned over, all systems shut down. This malfunction caused the liquid

solutions being produced to freeze, causing them to destroy the pipelines they ran through.

This disaster cost the company over $1 million in new equipment. The catastrophe caused

massive delivery delays to their customers, and the company believes numerous customer

accounts were lost as a result. This is just a small example of what could happen when

computer software and related equipment is not tested for Y2K compatibility. Now,

imagine the confusion and disaster that could result from a similar incident occurring in a

hospital–where lives, not inventory, are at stake.

" Code Blue 2000" is the term used to describe the possible breakdown of the

world's hospital software and related medical devices. Most hospital organizations have

prepared themselves for any problems that might occur with their software and medical

equipment. It is the organizations that ignore the potential problem that will most likely

loose valuable patient information, and in extreme cases, have their ability to furnish

adequate health care reduced.

Major Hospital in Shelbyville, Indiana, has a team of computer scientists currently

testing the hospital's computer system's software for Y2K compatibility. First, mock

systems are tested to determine what will actually happen when the year changes. Then,

obsolete software and equipment is replaced with Y2K compliant equipment. Major

Hospital has spent over a half-million dollars on research of the Y2K problem. This

research is extremely costly to an organization, but the alternative–ignoring the

problem–could be catastrophic.

This report will cover the numerous ways the Y2K problem could affect hospitals.

The first and most important area that will be reviewed is the manner in which the Y2K

problem could affect patients. The Y2K problem could adversely affect the biomedical

devices some patients rely on for life-sustaining purposes. Then, the potential problems

on the clerical side of hospital administration will be explored; focusing on patients'

medical records and accounts. Finally, the possible adverse effects on utilities such as

electricity, gas, and water will be discussed. A hospital is a place that a person should feel

safe and secure. This report will describe the steps being taken by hospitals to ensure that

their patients' peace of mind and sense of security is unaltered.

The Y2K problem is a concern for hospitals worldwide for a variety of reasons.

Perhaps the most pressing concern are the biomedical devices, which contain computer

software, that many patients rely on. Some critical biomedical devices are pacemakers,

fetal monitors, Magnetic Resonance Imaging machines (MRI's), and heart defibrillators.

One of the most important biomedical devices that could be affected by the Y2K

problem is the pacemaker. A pacemaker is a biomedical, electronic device implanted in

the wall of the heart designed to detect irregular heartbeats and provide regular, mild,

electric shocks that restore normalcy to the heartbeat. The pacemaker then records the

time an electric shock was administered; this information can then be downloaded to a

computer system and analyzed by medical personnel. Cardiologists use this information to

detect patterns and irregularities in the patient's heart rhythms. If the software were to

record faulty times for the shock deliveries, the cardiologist could misinterpret the results

and administer improper medical care. The results could be deadly for some patients.

The Veteran's Administration interviewed the top five pacemaker manufacturers to

gauge their awareness of the potentially hazardous Y2K problem. One company said the

problem would be corrected by mid-year; two companies stated the problem was already

under control; and the final two companies were behind schedule in eradicate the problem.

In addition to the pacemaker, there are several other biomedical devices that may

contain faulty software. One such type of device is an anesthesia monitor. An anesthesia

monitor regulates the anesthesia's effect on the patient during surgery. Another critical

biomedical device is a fetal monitor. A fetal monitor helps examine the condition of the

baby while it is still being carried by the mother. Incubators, critical to a newborn baby's

survival, could also be adversely affected by the Y2K problem. Other biomedical devices

(and their functions) include MRI's (produce computer-generated views of arteries,

nerves, tendons, and tumors), infusion pumps (used in intravenous drips), and heart

defibrillators (emergency method of establishing a heartbeat). All of the aforementioned

devices contain embedded microchips critical to their functions. There are also intensive

care monitors that may not be Y2K compliant; these include heart monitors, blood

pressure monitors, and machines that provide additional oxygen and physical support.

Finally, dialysis machines (help remove waste from a patient's blood) and radiation

equipment (x-rays, chemotherapy, etc..) are other critical pieces of medical equipment that

could fail if the software controlling their functions is not Y2K compliant.

Major Hospital is currently working with all of their medical equipment vendors to

ensure that all biomedical devices are Y2K compliant. " We are confident that outstanding

patient care will not be interrupted," says Carol Hussman, information systems manager at

Major Hospital, " and we are about 95 percent finished with all testing."

One may think that in this day and age, with all of our technological advancements,

that the Y2K problem would not be of concern to even the average computer user with a

fairly new system; much less a vital institution such as a hospital where thousands of our

loved ones lives hang in the balance. However, this is not the case. There are still

hospitals in the United States that are not equipped to deal with the Y2K problem.

Moreover, the U. S. is not the only place where the Y2K problem is causing difficulties. In

fact, almost a third of computer-related equipment in Australian hospitals, including

cardiac monitors and drug distribution systems, have failed the millennium test.

The final aspect of patient care that may be affected is the mental health of the

patients. In a crisis situation, patients might panic; hospital staffs will have to be aware of

this potential crisis. Major Hospital personnel are aware of this aspect of the Y2K

problem and are focused on preventing any software problems that may lead to patient

confusion or panic. However, there are no specific strategies in place to handle possible

patient disorder, other than by answering patient questions on an individual basis.

The Y2K problem is not limited to biomedical devices, however. This dilemma

effects non-medical devices such as the personal computers used in record-keeping and

accounting. If the programs that are used are not corrected, many problems could arise.

Even though some patient records are kept in paper form as a backup, most patient

information, such as test results, medical histories, registration, and insurance information

are kept in computer databases. These databases, if left unchecked for the Y2K problem,

could malfunction. Patient information is important to physicians and other hospital

personnel using the databases. It is readily available to them at the touch of a keypad. If

patient information is inaccurate, it could result in detrimental care or incorrect medication

being administered to patients.

This dilemma could be solved in one of two ways. One option hospitals have is to

put all information on paper, which would be very time consuming and prone to cause

errors, or the database systems can be programmed to be Y2K compatible. In order to

address the Y2K problem, President Bill Clinton signed into law the " Year 2000

Information and Readiness Disclosure Act." In a statement by the president released by

the Office of the Press Secretary of the White House, this law requires the shared

" necessary information tools needed to overcome the Y2K problem." This will help

hospital information systems departments acquire the knowledge necessary to reprogram

noncompliant systems.

The personal computer problem not only affects the hospital records department,

but also the purchasing, billing, and payroll aspects of the accounting department. The

purchase of essential medical equipment and supplies could be delayed if clerical software

is not brought into Y2K compliance.

In addition to President Clinton signing into law requirements that hospitals and

other businesses share information to help solve the Y2K problem, The Washington State

Health Association (WSHA) also recommends steps for compatibility for insurance billing.

According to Tom Byron, chief information officer of the WSHA, " The Washington State

Uniform Billing Committee (WSUBC) has adopted multiple resolutions concerning

electronic submission of Uniform Billing (UB-92) claims such as, (1) use of the Medical

Flat File, Version 5. 0, (2) all plans should be ready to accept the recommended format by

October 1, 1998, (3) providers should submit claims in the recommended format by

January 1, 1999, (4) all plans should allow for a period of October 1, 1998 to March 31,

1999 for providers to submit claims in either the recommended format or the current

format, and (5) electronic formats not Y2K compliant should cease beginning April 1,

1999. If the laws enacted by the U. S. Congress and the president , and the

recommendations made by the WSUBC are followed, the Y2K problem will likely have

little or no affect on the clerical areas of hospitals.

In addition to the patient care and clerical concerns facing hospitals with respect to

the Y2K problem, there is one other pressing concern for hospitals. Utilities are essential

to the everyday life most people are accustomed to. If the electricity goes out at home,

most people just burn candles and wait, without much worry, for the lights to come back

on. However, losing utility service in a hospital could be much more than an inconvenience.

Imagine having to go to the hospital on December 31, 1999. It could be more of a

problem than you think. All hospitals rely on electricity, gas, and water for their everyday

operations. A spokesperson for Major Hospital states that all methods have been

exhausted to comply with state and federal guidelines and suggestions regarding the Y2K

problem. The suggestions include, but are not limited to, obtaining a copy of the

" Approach to the Y2K Problem", distributed by the federal government. This approach

suggests a plan of attack and an inventory of all systems that might be affected. A team

should be formed with a leader to assess the problems. This team should assess and

prioritize possible problems. At that point, the team must prepare a list of all assessments

made. This leads the team to the testing phase of the operation. After testing, corrections

should be made, and a reassessment needs to be done. Utilities are just a small portion of

the testing that will be done.

Utility companies are spending more than $2 billion to test and prepare their

computers and replace software in order to successfully meet the Y2K challenge. At this

time, there is no evidence that the Y2K problem will create power failures within the

nationwide electrical power-service grid. Electric companies plan to have a dress

rehearsal in September, 1999, to gauge how utilities will react to a simulation of the Y2K

scenario.

The inability of some equipment and computers with date-sensitive components to

distinguish the correct year after the year 2000 has now become a widely recognized and

accepted problem. The utility company Cinergy began an active response to this dilemma

in 1996 with a review of several million lines of computer software application code in a

campaign to locate and correct date-sensitive fields. Most of that code has since been

examined, corrected, tested, and returned to operation. All such remaining systems are on

schedule for completion by March, 1999.

Cinergy, like most owners of information systems, will be required to modify

significant portions of its systems to accommodate new local, state, and federal

requirements brought about by the Y2K problem. During 1997, Cinergy incurred costs of

approximately $8 million. Maintenance or modification costs will be absorbed as they

occur, while the costs of new software will be capitalized and amortized over the

software's useful life.

For example, at Hawaiian Electric Company (HECo), the Y2K project team

identified significant problems with its energy management system (EMS). EMS is the

" brain" of the power distribution system at all electric companies. This system is used to

remotely control transmission system breakers, coordinate power generation schedules,

compensate for large transmission line breaks, and provide protection against voltage, and

current and frequency transients. HECo and their EMS system vendor determined that

EMS would crash on the rollover to January 1, 2000. This would have, in turn, resulted

in HECo's transmission network crashing, and by default, a major power outage and loss

of all generating capacity.

Besides medical devices, embedded chips are " hard wired" into other pieces of

equipment that may be critical to patient services or hospital operations. This equipment

is often the responsibility of the vendor, not the hospital. These systems include 1) fire

alarm systems, including detection, sending/ receiving, and suppression units, 2) security

systems, including sending/receiving units, video and surveillance systems, and badge

readers, 3) telecommunications equipment, including telephone switching equipment,

emergency call management systems, pagers, and cellular phones, 4) building

infrastructure, including HVAC, energy management and lighting controls, emergency

generators and lighting, uninterruptible power supplies, and elevators. Major Hospital is

among a number of the world's health care providers that will participate in every effort to

minimize any and all malfunctions related to the Y2K problem.

Gas companies are contacting their suppliers and service providers to determine

the status of their year 2000 compliance projects and will be developing contingency plans

if their efforts do not meet certain goals. An inventory of computer systems, embedded

systems, and resources has been developed and prioritized according to the importance to

the continuing operation of the companies. It is anticipated by gas

companies that this

testing, and any required modifications to systems, will be completed by July,

1999.

Major Hospital uses gas for heating and lab equipment. However, Major

Hospital is

unlikely to be affected by a gas outage because gasoline-powered electric

generators will

take over in the event of an outage and run most systems.

Wastewater and sewage treatment facilities are highly automated and

contain year

2000-vulnerable embedded chips. Also, emissions monitoring and control

systems depend

on year 2000-vulnerable embedded controls. Malfunctions due to Y2K

problems could

lead to accidental pollutant-filled releases and emissions that could

endanger local

residents. In August, 1998, a malfunctioning computer in Boulder, Colorado

was blamed

for water main breaks that cut service to over 40 homes, flooded basements

and garages,

and turned city streets into raging rivers. A computer controlling water pressure gave

inaccurate readings, prompting a city worker to open the mains. Some residents and

businesses were left without water for over a week. Major Hospital staff have prepared

for a water shortage. They have stocked up on bottled water, just as every other hospital

has done. However, bottled water will only last so long. In the event of a prolonged

water shortage, such as the one in Boulder, Major Hospital personnel will be faced with

personal hygiene and medicine issues. Patients must be bathed on a daily basis and

washed off completely. It is difficult to comprehend a hospital as an unsanitary

environment; where doctors must " scrub" repeatedly to reduce the risk of infection and

patients must be kept free of germs. Medicines are sometimes mixed with water to form

their completed structure. This crux could alarm the many patients who depend on these

medicines. The sewage treatment plant in Shelbyille, Indiana that services Major Hospital

states that the plant is already Y2K compliant.

The faculty and staff at Major Hospital is extremely confident that when the new

millennium arrives, it will not be accompanied by any significant problems or catastrophes

with regard to malfunctioning utilities. If any problems do surface, Major Hospital has

assured its community and its patients that the problems will be minor in scope and will be

quickly and efficiently dealt with.

As has been discussed in this report, the Y2K problem is a vast and complex issue

that must be dealt with by hospitals. Virtually every facet of hospital care is affected by

the Y2K problem. Patient care, clerical software, and utilities are three major aspects of

the hospital organization that, if left unchecked for Y2K compliance, could cause

confusion, sickness, and even death among hospital patients. Worst case scenarios involve

malfunctioning pacemakers, improper medication being dispensed, and unusable

defibrillators in emergency situations. The Major Hospital staff, like most other hospital

staffs, continues to work diligently to ensure that whatever malfunctions occur are minor.

It is difficult to predict the scope of the Y2K problem and the possible severity of

related malfunctions when the most knowledgeable computer experts disagree on the

severity of the problem. According to Alastair Stewart, a senior Year 2000 advisor with

information technologies market watcher Giga Information Group, the Y2K computer

date bug will not cause an " embedded systems Armageddon" as some have feared. " It

may rain, but the sky won't fall." Giga recently called for a " common-sense approach" to

the Y2K threat. Some projected scenarios have Y2K failures toppling civilization. For

example, in one sequence of falling dominoes, embedded track switching controls will

cause railroads to fail to deliver coal to power generation plants. As a result, electric

utilities–which have Y2K problems of their own–will shut down. As the power grid goes

dead, telephones will stop working. Without communications the interlinked banks and

international finance structures begin to fall and, ultimately, so does civilization.

" Can you hear the four horsemen galloping off in the distance?" remarked Stewart.

" It's easy to scare people with talk about The Great God Teowawki." " Teowawki"

stands for " the end of the world as we know it," Stewart explained.

Just as some downplay potential Y2K problems, others offer substantial evidence

that the Y2K problem is for real. Mike Wedland, a noted software expert and author of

numerous computer software guides, produces the following examples for consideration:

U. S. Social Security computer programmers have identified 30 million lines of code

that need to be changed to reflect the correct date after the year 2000. Some 400

programmers have been working on this problem since 1991. As of June, 1997 they

had corrected only 5 million lines.

The Internal Revenue Service has identified 100 million lines of code that need to be

changed in their computers to fix Y2K problems. They have only found about 300

programmers and they are just now getting started.

An estimated 65 percent of the businesses in the U. S that need to correct the problem

have done nothing so far.

Regardless of whether the Y2K problem is all hype or a catastrophe waiting to

happen, hospitals must prepare for the worst. While businesses deal in profits and stocks,

hospitals deal in human beings. When peoples' health and lives are at stake it is best to be

aggressively cautious. It appears that most U. S. hospitals have a firm understanding of the

consequences of not being Y2K compliant, and are dealing with the issue accordingly.

Word Count: 3352