DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Food and Drug Administration
9200 Corporate Boulevard
Rockville MD 20850

SEP 2 1 1998

• Dear Medical Device Manufacturer:

I am concerned, as I am sure you are, that failure of computer systems due to Year 2000 ("Y2K") problems could disrupt the production and supply of important medical products. This in turn could have serious implications for patient care. I am especially concerned about high volume, consumable and single-use medical devices, as well as in vitro diagnostics, where disruption of operations for one or a few major manufacturers could create significant shortages.

This letter is intended to elaborate on some of these concerns, to suggest some basic actions addressing the Y2K problem, to explain the regulatory framework that underlies those actions, and to enlist your help in avoiding disruptions in healthcare delivery. I know that many of you take the Y2K issue seriously. You are conducting extensive Y2K analyses and are planning, implementing, and validating changes in your business systems, manufacturing operations, and record keeping. I want to be sure that all manufacturers share that sense of obligation.

Complexity of the Y2K problem

The Y2K issue affects more than just date-related functions. For example, many computer chips used in automated systems include an internal clock, which may be used for certain timing applications. If they are not Y2K compliant, these chips can behave unpredictably on or after January 1, 2000, and computer applications using these chips can fail if they do not properly handle information from the internal clock. Furthermore, some analyses have shown that even when a chip is not used for a date function or for timing purposes, a failure of its internal clock might still adversely affect the computer.

Another issue is the increasing level of integration, networking and interdependency among automated processes, such that Y2K failure of one automated application can have widespread impact on other operations. For example, automated equipment is widely used and interconnected in many aspects of medical device manufacturing, including design, laboratory operations, material control, quality assurance, testing, record keeping, document control, production processes, and device distribution. Plant floor operations can involve extensive use of embedded systems in programmable logic controllers, digital function controllers, statistical process control, supervisory control and data acquisition, robotics, human-machine interfaces, input/output devices, and computer operating systems.

These and other factors make it very difficult for firms to fully assess their Y2K vulnerability. To accomplish this, device manufacturers often need assistance and

cooperation from third-party vendors of their automated equipment, and from suppliers of their components and services. Some vendors/suppliers may not promptly and forthrightly provide Y2K information because of their own incomplete Y2K assessment and because of legal and liability concerns. Moreover, suppliers often face the same Y2K issues and difficulties from their own suppliers, resulting in a potential "domino effect" in supply and distribution chains.

Regulatory framework for Y2K actions

The Y2K problem is unique in that it has been predicted and identified as a significant cause for concern long before it may become manifest. However, now that the potential problem is known, device manufacturers have a regulatory obligation to properly address theY2K issue–the Quality System regulation (21 CFR 820.100) is clear regarding the obligation for firms to take corrective and preventive actions. The regulation is also flexible, providing wide latitude for you to take the steps needed to avoid non-conforming devices or serious quality problems. At a minimum, you must analyze your processes and work operations to identify both existing and potential causes of non-conforming devices or other quality problems, and then take action to correct problems and prevent their recurrence. Such actions must be verified or validated to ensure that they are effective. The Quality System regulation (21 CFR 820.70(i)) also requires that when used as part of production or the quality system, computers and automated data processing equipment must be validated for their intended use (including proper operation on or after January 1, 2000).

Taking action to address the problem

To help you in assessing and correcting your manufacturing operations and quality system software, there are a number of information resources available. For example, a search of the World Wide Web reveals numerous articles regarding the Y2K problem for embedded industrial systems. The following are a few helpful Web sites, which contain extensive links to other Web sites concerning embedded systems:

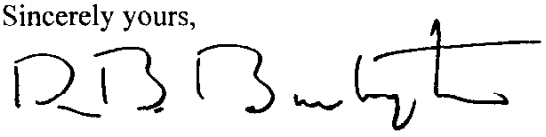
National Institute for Standards and Technology	http://www.nist.gov/Y2K/
World Bank	http://www.worldbank.org/Y2K/pages/english/eemb.htm
Institution of Electrical Engineers (U.K.)	http://www.iee.org.uk/2000risk/guide/home.htm
British Columbia Government	http://www.Y2K.gov.bc.ca/enbedsys.htm
General Accounting Office	http://www.gao.gov/special.pubs/bcpguide.pdf

While there are many actions that can be taken to address the Y2k problem, several are common in the information that we have reviewed. These include:

- Inventorying all automated systems used in any aspect of your operations.
- Prioritizing those systems based on their criticality to continued operations.
- Seeking Y2K status information from equipment and software vendors.
- Determining whether the Y2K information provided is accurate or detailed enough to satisfy your needs.
- Undertaking Y2K testing, mitigation or replacement as needed, especially for the most critical applications.
- Contacting component and service suppliers to assess their vulnerability to a Y2K disruption.
- Developing contingency and disaster recovery plans, including manual backup procedures for automated in-house operations, alternative sources of supply for components and services, holding additional inventory of supplies for transitional use, and possible strategic replacement of mission critical equipment for which Y2K status cannot be adequately assessed.

I trust that you are already taking action to investigate and address this issue. If Y2K obstacles present the potential for significant quality problems or medical device shortages, we want to know as early as possible. I welcome your feedback and any suggestions regarding this issue, including what assistance is needed from the FDA. If you have suggestions or anticipate production disruptions, please contact Stewart Crumpler in our Office of Compliance at 301-594-4659, or via FAX at 301-594-4672.

Sincerely yours,



D. Bruce Burlington
Director
Center for Devices and
Radiological Health