IS Disaster Plan

Disaster planning is one of the most important things a hospital Information Systems department does. Not only is the Information Systems department subject to all the normal outages – due to fire, flood, natural disaster (earthquake, tornado, etc.), civil disturbance, etc. – that all businesses are subject to, but there are two very important differences. First, in a disaster, a hospital will typically get more admissions (e.g., influx of emergency casualties), experience high census, and must respond to the needs of the community in ways that put high stress on systems. Most other businesses can just shut down during these critical periods, while a hospital must continue running, and at a higher capacity. Second, the nature of information systems and computers makes them susceptible to other forms of "self-contained" disasters that have widespread repercussions. For example, a hard drive crash on the hospital mainframe system is a "disaster" contained only to the few square inches of the drive. But its devastating effects are felt throughout the organization when systems that are relied upon for patient care and communications are no longer available. Having a robust and effective Disaster Recovery Plan in place helps to preserve the institution's health care services that the community relies upon, and protects its continued business and financial viability.

Scope:

The disaster recovery strategies described in this section outline the plans for the MNGH's information systems. In a hospital-wide emergency, the hospital's Disaster Plan will always take precedent over this plan; this plan should be considered a sub-plan of the hospital's overall disaster plan. MNGH's Command Team will organize and manage the MNGH facility response to business interruptions and associated problems. The MNGH Command Team will serve as a clearinghouse for business recovery related communications, and will invoke departmental disaster recovery plans as appropriate. However, the Information Systems disaster plan may need to be activated even when the hospital as a whole is not in a state of emergency and/or the hospital-wide disaster team is not activated, such as when responding to "self-contained" IS disasters. Systems interruptions and outages, no matter how minor, need to be rectified expediently so as not to disrupt patient care.

Information systems disaster planning is guided by two major principles:

1. Prevention – The Information Systems department takes steps on a continual basis to prevent systems interruptions and outages.
2. Downtime Procedures – Hospital-wide procedures must exist for periods of information systems downtime.

Prevention:

UPS: All MNGH servers and communications equipment (hubs, routers, etc.) are connected to uninterruptible power supplies (UPS). Additionally, all UPSs are plugged into the hospital's emergency generator power outlets (red plugs). In the event of a power outage, the UPS maintains electricity to the servers and equipment during the period of switchover to generator power. The current UPSs on the MNGH-based servers can maintain uptime for approximately 10 minutes at full load; however only 10 seconds or less is needed during the switch-over period. Generator power can be provided indefinitely depending on fuel re-supply capabilities (at least 4½ days with on-site fuel supply). The Nortel Phone System is also connected to a UPS which is connected to emergency power. The hubs and electronics in each communications closet on each floor of the hospital are also connected to UPSs which are connected to emergency power.

Backups: Data backups onto tape are done for each server on a regular basis. Daily backup tapes from MNGH-based servers are kept on the 8th floor, in a locked heavy-duty metal cabinet, behind a pad-locked door. Monthly backup tapes are kept off-site in a secured vault maintained by Arcus Security/Iron

Mountain (beginning July, 2000). Daily backups are re-used after one month (4-week tape rotation). Monthly backups are kept for 12 months before being re-used. Documentation of backups (schedules, tapes, procedures, record-keeping) are kept in the IS department. Periodically, tests are done of restoration of data to ensure that the data contained on the backup is viable. Backup media are routinely replaced when specified usage limits are reached or when media errors warrant. IS staff cleans the tape drives on a routine basis (at least monthly).

Fire Control: An overhead fire control sprinkler system has been completely implemented throughout the hospital including the IS computer room, the Nortel phone system closet, and communications closets. This system delivers water only to the areas specifically affected by fire; thus limiting the amount of water damage. Emergency six-inch water drains are in place throughout the hospital. A main 16" drain exists to control basement flooding. All computer and telephone equipment is raised above floor level for possible local flooding.

Metro ISD: Several systems used by MNGH are located off-site at Metro ISD (Howard School facility). These systems include Affinity, Blood Bank, FastNet, and Internet access. The Data Center at Metro ISD is protected by UPSs, generators, and fire control systems. The fiber communications link between MNGH and the Metro ISD facility has some redundancy, so that the link can be maintained even if one side of the fiber cable pair is cut.

Downtime Procedures:

The importance of downtime procedures cannot be over-emphasized. Even if a disaster (hospital-wide or "self-contained") never hits, computer systems often need to be unavailable during times of routine maintenance, upgrades, etc. It is important that all computer users know what to do - how to continue doing their jobs – when the computer system is unavailable. Too often, the fact that "the computer is down" is used as an excuse for users not doing their jobs. Each hospital department and/or work area must take responsibility for documenting downtime procedures. These procedures must be written and maintained within each department in a binder that is readily accessible to managers and staff. Staff should be knowledgeable about downtime procedures, and practice them regularly to ensure that users are adequately trained.

There are two different types of downtime procedures. One set of procedures can often be used when computer downtime is of short duration (one day or less) and is known ahead of time. This is typical of a planned temporary outage due to routine maintenance or upgrades, or possibly the "self-contained" disasters that are readily fixable. Another set of procedures might be used when the downtime is unexpected and is of an extended nature (5 or more days), such as might occur in an actual hospital-wide disaster (fire, flood, earthquake, tornado, etc.). Staff training, education, and documentation of procedures in each of these events are crucial.

For each of the downtime events – short duration or prolonged – a plan must be put into place for not only how the jobs get done without the computers, but how recovery takes place. Each of these will likely entail additional temporary staff to assist in handling extra daily workloads for the outage period and for catching up on the entry of data into the computer systems after normal operations are resumed. Depending on the length of downtime, the catch up once the systems are back online can be very labor intensive and time-consuming. Synchronizing data may be difficult. These are all points that must be carefully documented in downtime procedures, including approvals for overtime, additional staffing, and the like.

Emergency Planning:

It is essential that the contents of any disaster, emergency preparedness, or business recovery plans be communicated to all personnel so they know from a departmental and an individual basis what their role is in various disaster scenarios. Copies of disaster plans should be readily available in each department. A copy of this IS disaster plan should be stored in the Information Systems department, in the MNGH Executive offices, on the 8th floor of hospital in the heavy-duty locked metal cabinet which houses the backup tapes, and off-site at Iron Mountain's secure vault facility (in case the hospital facility itself is uninhabitable and/or occupancy is not possible for a period of time during the emergency). Included with this document should be up-to-date documentation of:

- Inventories of computer hardware and software,
- Key vendor, supplier and business contacts, including those for off-site facilities such as the PCC and key financial institutions
- Contacts for the MNGH Board of Directors, executive leadership team, and department heads
- Contacts for relevant Metro government agencies and departments, such as the fire department, Metro's Office of Emergency Management, TDOT, and others
- Contacts for relevant state and federal agencies, such as State of Tennessee's Office of Emergency Management, and others
- Network diagrams which document the location and connectivity points of the data and communications infrastructure
- Facility diagrams, which document the physical plant and locations of any hazards.

These disaster and emergency preparedness planning documents should be updated at least once yearly. Institutional resources need to be specifically allocated, tracked and accountable to MNGH's Executive Management to ensure that the business recovery plan is kept current.

In an actual emergency, a Command Center will be established. This will provide a predetermined place where MNGH's Executive Management the leaders of the various recovery teams (hereto referred to as the Command Team) can meet to coordinate recovery team activities. Special phone jacks, extra phone instruments, a FAX machine and hand-held communication devices need to be planned and available in advance so that necessary communications can be activated without delay.

The MNGH Command Team will lead the MNGH facility in responding appropriately to problems and issues related to business disruptions in order to deliver quality patient care in a safe environment and to preserve the business integrity of the institution. Input by the Director of Information Systems, the Director of Patient Services, the Director of Facilities Management, the Chief Operating Officer and the Chief Financial Officer, is crucial to successful management and recovery activities. The MNGH Command Team will facilitate communications to hospital staff, the PCC, Our Kids, the MIC, medical staff, other hospitals and the Nashville Metropolitan Office of Emergency Management as appropriate. This team will work closely with the Director of Community Development and Public Relations regarding the specific business interruption and related events to ensure that there is one coordinated point to disseminate information to the media.

Notification about any irregularities or problems with equipment, utilities, communications or supplies that may arise due to business interruptions may come from staff, department managers or division heads in the form of telephone contacts, e-mails or direct communications. Notification involving information systems – either directly or indirectly – should be made to the Director of Information Systems. The IS Director will investigate and evaluate the problem, and determine whether the IS Disaster Plan should be invoked, and/or may invoke the assistance and cooperation from other departments or Metro business entities (such as Metro ISD). Likewise, emergencies in other departments and/or Metro business entities may cause need for the involvement of the MNGH Information Systems department.

Call List:

In the event of an emergency affecting information systems, the call list shown below should be used as a means of organized notification and communication. The call list should be regularly updated and maintained in a place of ready access by all IS staff – both at home and at work. This call list should also be part of the hospital's overall disaster plan, and be available at all times to the MNGH Command Team.

IS Disaster Scenarios:

A. MNGH Computer Room Destroyed

Systems Affected:

- CCA – Lab and Pharmacy (HP 9000)
- Kronos Timekeeper and Gatekeeper Systems (PC-based)
- Exchange Email System (PC-server)
- Novell Network (PC-server), including many server-based application such as Employee Health, PerSe One-staff (nurse scheduling), Horizon Medical Credentialing
- HBOC Materials Management (PC-server)
- Connectivity to systems at Metro ISD (Affinity, Blood Bank, FastNet, Internet access). Note: although the systems at Metro ISD may not be down, the fiber link connecting them to all the hospital floors runs through the MNGH Computer Room. Thus, these systems will appear "down" to the users, because they will be inaccessible.
- Off-site locations, such as the PCC will be unable to access the MNGH-based systems; however they would still be able to access to systems at Metro ISD because they have an independent fiber connection to Metro ISD.

B. Metro ISD Computer Room Destroyed

Systems Affected:

- Affinity System (Aviion 9500), including Patient Registration, Patient Accounting, Patient Scheduling, Order Control, Medical Records, DRG, Medical Records Abstracting, Master Record Index, Medical Records Control, DM (Radiology Dept. Mgmt.), General Ledger
- Sigma Blood Bank System (MV 10000)
- Fastnet Financial System (IBM AS400), including General Ledger, Accounts Payable, Payroll
- Internet access (PC-servers), including external email
- Off-site locations, such as the PCC, will also be affected by inability to access the above systems

C. MNGH Main Phone Closet Destroyed

Systems Affected:

- Nortel Phone Switch
- ATM Fiber Link to Metro ISD. This is the point of entry into MNGH of the fiber communications link. Thus, all the systems described in **B** above will be inaccessible and will appear to be down. If this happens, the expedient thing to do is to relocate and re-terminate the fiber entry into MNGH. As long as the fiber can be brought into the MNGH Computer Room, it can be distributed throughout the hospital via the existing communications closets.
- Communications Multiplexer link to Our Kids (which connects Our Kids to the Affinity system).
- MNGH Paging System
- MNGH Beeper System
- Off-site locations, such as the PCC will be unable to access the MNGH-based phone system; however they would still be able to access to systems at Metro ISD because they have an independent fiber connection to Metro ISD.

D. MNGH Power Outage

All MNGH systems outlined in **A** and **C** above would be affected. However, because of the UPSs and backup generator (described above - see Prevention) systems will continue to be operational. The main problem with a hospital-wide power outage is that not all end-user devices (PCs, terminals, and printers) will be likewise protected. Most will be down. However, there should be at least one device in each department or critical work area that is (or can be) plugged into a red outlet (on generator power). Identifying this device, ensuring it is plugged into the correct outlet, and documenting this in the downtime procedures, is the responsibility of each department manager.

E. Metro ISD Power Outage

All systems located at Metro ISD outlined in **B** above would be affected. However, because of the UPSs and backup generator (described above - see Prevention) systems will continue to be operational. The main concern would be the length of the power outage. Whereas MNGH has generator fuel for 4½ days, Metro ISD has capacity only for 20-hrs. (with a 12-hr. fuel re-supply commitment). Selective systems may need to be brought down at selected times to conserve fuel. Communications dialogue between Metro ISD and MNGH's Director of Information Systems is critical during this period.

F. Fiber communications lines cut between MNGH and Metro ISD

Connectivity from MNGH to all systems located at Metro ISD outlined in **B** above would be affected. Communications dialogue between Metro ISD and MNGH's Director of Information Systems is critical during this period. Metro ISD will facilitate enlisting the assistance from other Metro departments to get the fiber link re-established.

G. MNGH basement flooded or damaged by fire

All MNGH systems outlined in A and C above would be affected. In addition, Facility Environmental Computer Management Systems, the Johnson Controls heating and air conditioning systems, and the Pneumatic Tube Control System would also be affected. For these systems, refer to the disaster plan within the Facilities Management department. If the downtime is expected to be extensive, the environmental impact (no heat/air) may require relocation or evacuation of patients and the possible closing down of the hospital. This effort would be directed and managed by the MNGH Command Team.

Disaster Procedures:

Should a disaster strike, such as one of the scenarios described above, the following procedures should be implemented:

1. The MNGH Director of Information systems should be alerted. If the Director cannot be contacted, begin contacting the others on the IS call list in order.
2. The MNGH Director of Information Systems (or the senior-most IS staff member contacted on the call list) will alert the Chief Financial Officer and/or the MNGH Executive Leadership Team of the situation.
3. If appropriate, off-site facilities such as the PCC will be contacted to alert them of the situation.
4. Activate the Hospital-wide Disaster Plan, and the MNGH Command Team, if appropriate. Alert MNGH Security to preserve order surrounding the damaged area in the facility and the building perimeter, if appropriate.
5. Retrieve disaster plan documents (such as this plan), network diagrams, vendor and business contact lists, and documentation of computer hardware and software, from one of the stored locations.
6. MNGH Command Team will contact key business partners to alert them of the situation.
7. Activate a team to do damage assessment. Depending on the nature of the disaster, this team might include the Information Systems Director, Network Manager, Applications Manager, Metro ISD

contacts, the Director of Facilities Management, and/or selected members of the Executive leadership team. The purpose of this team is to determine the extent of the damage and provide executive management with an initial estimate of the impact on business activities, the expected duration of the problem, the possible timeframe for recovery efforts, and estimates of restoration resources and costs.

- If disaster includes a power outage (either at MNGH or Metro ISD), obtain assessment of power problem from NES and inform Metro and MNGH Command Teams with initial estimate of impact on Metro and MNGH business activities and provide initial estimates of restoration timeframes.
- If disaster includes damage to the fiber communications link between MNGH and Metro ISD, Metro ISD and MNGH IS damage assessment teams to assist communication's vendor with determining extent of the damage and alternatives for re-routing of data communications. Damage assessment teams to provide initial estimates of restoration timeframes and costs and work with the communication vendor for emergency repair and support requirements.

8. MNGH Executive Management Team to determine if damage impact to essential hospital systems severe enough to warrant temporary closure of the hospital. If so, relocation of patients and staff is to be initiated and coordinated through the predefined agreement established with other local hospitals.

9. Determine if cold site at Metro's Howard School will be utilized on a temporary basis or if the MNGH computer room will be renovated quickly enough to avoid an intermediate site installation or if an alternate site within the hospital could be used (see **Recovery of Operations** below). If disaster was at Metro ISD, determine if MNGH computer systems located at Metro ISD (Affinity and Sigma) could be moved to MNGH's computer facility or if restored/replacement systems should be relocated to MNGH's computer facility rather than re-installed at Metro ISD (see **Recovery of Operations** below).

10. IS recovery teams and key vendors will identify replacement/repair equipment requirements. Prepare and obtain approval for emergency replacement/repair requisition orders and acquire required funding. If the systems affected were the responsibility of Metro ISD (FastNet, Internet access, fiber communications link) Metro ISD will contact key vendors and business partners, and will prepare and obtain approval for emergency replacement.

11. If phone systems are affected:
    - Activate 25 emergency phones and deploy hand held "walkie talkies" to key areas in the hospital.
    - Activate temporary personnel to act runners, which may need to be employed to facilitate communicate between departments.

12. If the nature of the disaster involves basement flooding, MNGH Facilities Management will isolate and cap off any break in the hospital's water system to stop any uncontrolled flow of water, and will acquire and activate emergency pumps in the critical service areas in the basement. Note: In the event of a fire, water from the Fire Department's effort to quench a fire on upper floors will inevitably flow to the basement. Critical facilities located in the basement include:
    - IS computer room
    - Main power panels
    - Emergency power generators
    - Heating and air-conditioning control systems
    - Main phone closet and communications room
    - Vacuum systems
    - Refrigeration systems
    - Elevators
    - Food service area

    Facilities Management with the assistance of outside vendors, if necessary, will begin drying out and cleaning up essential service areas. Food service damage will need to be evaluated and if necessary, an alternative outside source of food service to patients and staff will be obtained.

13. Public Relations Team briefed. Establish communications as soon as possible with Metro government agencies including the mayor's office, the media, Metro's Office of Emergency Preparedness, and other hospitals in our joint emergency agreement (for patient evacuation and relocation), as appropriate.

14. MNGH Facility and IS Recovery teams to initiate cleanup and restoration of computer room facility and network connectivity. Outside vendors employed to assist in restoration activities, as appropriate.

15. IS Recovery Team to initiate installation of temporary equipment work-arounds for partial restoration of computer and network capabilities, if feasible. Determine if locally stored backups (8th floor) can be utilized or whether off-site backups need to be used. If off-site backups are to be used, specified individuals may contact Iron Mountain to request the necessary tapes. Tapes can be delivered within two hours.

16. In addition to having staff work longer shifts, suspending vacations, etc., extra staff may need to be called in during crisis periods to handle the extra workload created by the manual processes put into operation. Temporary personnel teams may need to be activated by Human Resource Department to assist MNGH departments on a 24 X 7 basis to operate as efficiently as possible during the outage period.

17. IS Recovery team will keep MNGH Command Team and/or executive leadership briefed on restoration activities. MNGH Command Team will in turn keep Public Relations Team briefed on restoration activities. MNGH's Public Relations spokesperson will keep media, other Metro government entities and the Nashville community informed of recovery efforts.

18. The IS Recovery Team will notify the MNGH Command Team and/or executive leadership that computer operations are restored. IS Recovery team and vendor representatives test and correct any deficiencies with the newly installed computer and network systems in the restored computer facility before going live. Selected departmental personnel may also be involved in this testing and/or setup.

19. If the phone system and/or fiber communications link was involved, facility and vendor recovery teams to certify that the restored main communication's closet is ready for occupancy and is ready for the installation of replacement equipment. Facility and vendor personnel will install replacement equipment for the network and phone switch systems, as needed. Test and correct any deficiencies with the newly installed phone switch and network systems before going live.

20. Knowledgeable MNGH, Metro ISD and/or vendor personnel verify that restored computer systems, and/or fiber communications link, and/or phone systems, and/or power systems are operating properly, prior to going live.

21. IS Department to coordinate with MNGH departments for the return to normal production status of computer systems as they become available. Have knowledgeable MNGH departmental personnel verify that restored departmental computer systems are operating properly and that the data updates were successfully completed. Department managers should oversee the verification process.

22. Communicate to all staff and off-site locations that the return to normal operations has been successfully completed. Coordinate return of patients if patient relocations were necessary. Coordinate required staffing to handle relocation of patients and the transition to normal hospital operations.

23. Public Relations Teams to notify media, other Metro government entities and the Nashville community of successful conclusion to the restoration process.

24. Manual records generated during the outage period may begin being keyed into the respective computer application systems. This may also include data previously entered into the computer system since the last monthly data backup was taken and stored off-site. For example: if the outage occurred on the 6th of the month and the backup from the previous end-of-month was used in

restoration efforts, the data for the 6 day period would have to be re-entered into the computer system (i.e., all data lost since the last backup would need to be re-entered). Additional staff and/or temporary staff may be needed.

25. If a temporary computer or phone system capability was implemented before the final restoration was complete, a move of the systems to the restored location(s) will be necessary. If temporary equipment was used to get operational quickly, IS and facility teams will need to continue to work with vendors to install permanent replacement equipment.

26. If phone system was involved, deactivate 25 emergency phones and return all hand held “walkie talkies” to Facilities Management department.

27. Data verification activities should be conducted through the first month-end process to assure accuracy of results.

Recovery of Operations:

Cold Site: If a disaster is confined to a limited area at MNGH (such as the MNGH server room being destroyed), the data center at Metro ISD can be used as a cold site. Temporary computer and communications equipment can be installed at Metro ISD. Usage of Metro ISD’s data center as a cold site is only practical if:

- outage of the MNGH servers affected and/or the MNGH facility housing them is expected to be longer than one-week
- no space within MNGH can be identified to serve as the “new” server room
- the fiber connecting the Metro data center and MNGH is unaffected or can be fixed within a short period (less than one week)
- the fiber network based out of the MNGH server room can be re-routed to another location within the hospital unaffected by the disaster
- the communications closets and PC/terminal devices in most of the MNGH facility are unaffected and in usable condition
- Metro ISD is unaffected and space is available within their data center

Affinity, FastNet and Internet access will immediately be accessible as soon as the fiber can be re-terminated within the unaffected portion of MNGH. However, servers that were housed in the destroyed portion(s) of MNGH will be inaccessible. These are various PC-based servers and the HP9000 CCA server (see above scenario of MNGH computer room destroyed). In this case, new servers will be ordered from vendors and setup at Metro ISD. Backup tapes can be retrieved from the off-site storage facility and restored onto the new servers. It is estimated that the PC-based systems could be operational within 10 days or less, the CCA system possibly longer.

If the disaster happened at Metro ISD’s data center, and the Affinity and/or Blood Bank servers were destroyed, but MNGH was unaffected, these systems could theoretically be replaced and housed at MNGH. However, replacing the older Affinity and Sigma platforms currently in use is problematic, since both platforms are not being manufactured any longer.

Affinity: It may be possible to locate an old, used Affinity server (Aviion 9500) on the used market. Problems are expected however, with reading the old tapes and restoring our current data. Tapes may need to be sent off to a vendor that can convert them onto “current” media. The existing operating system is no longer supported by the vendor and additional data translations (from Open/M to Cache) may be required. Downtime is expected to be extensive - one month or more - and the cost for data conversion is expected to be extremely high. A decision will need to be made whether to pursue recovery or to instead set up a brand new system from scratch with no historical data. The financial and patient care implications of this will need to be carefully weighed by the Director of Information Systems, the Chief Financial Officer, and others. If the Affinity server had been already moved onto a new platform as is being planned, then replacing the server and restoring the data would be a much easier proposition, and likely achievable within 10-14 days.

Blood Bank: It will be impossible to attempt to re-create our existing Sigma Blood Bank system. Not only is the hardware out of production, but the software is no longer being supported by the vendor. MNGH is already planning on purchasing a new Blood Bank system – which entails new hardware and software. If the new Blood Bank system had already been in use at the time of the disaster, replacing the server and restoring the data would be readily achievable within 10-14 days. However, if a disaster strikes prior to that time, the preferred method of recovery would be to step up the purchase and installation of the new system and start anew. Data from the old Sigma backup tapes could never be restored onto another system. Instead, just the blood bank index, which is currently being backed up monthly onto a PC, would be restored onto the new system.

FastNet and Internet: Maintaining these systems – including the disaster recovery planning – is the purview of Metro ISD, not MNGH.

Business Recovery Testing:

Simulated disaster drills and business recovery tests should be held yearly. Test objectives and simulated damage assumptions are established, documented and distributed to the testing team in advance of the test. Tests include pre-notification of the scope of the intended test to all MNGH departments. Surprise tests should also be conducted when appropriate. The tests cover:

- Activation of designated recovery teams – do team members know their roles?
- Are disaster manuals and associated documentation (key vendor and contact lists, network diagrams, etc.) updated and readily available?
- Are data and system backups retrieved properly and are they valid for recovery?
- Contact vendor(s) to verify emergency deliveries of replacement equipment and software for emergency delivery and installation assistance.
- Validate that effective and timely coordination takes place between participating the various business recovery teams.

Careful documentation is kept of events during the business recovery testing process to allow detailed evaluation and follow-up to remedy deficiencies that were encountered during the test. Meetings should be scheduled on a routine basis with Metro's Office of Emergency Management, Metro ISD and with MNGH's IS department. This will ensure that that emergency procedures are well understood by all parties and will be properly coordinated to ensure a smooth integration of resources in case of a major area disaster.