 <p>Heritage Provider Network &amp; Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-018	Effective Date: 04/20/2005	Page - 1 -
	Authored by: David Pfafman	Date: 01/11/2006	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Disaster Recovery Plan			

**POLICY:**

It is the policy of Heritage Provider Network to provide a plan to insure the accessibility of protected health information (PHI) in the event of data loss due to an emergency or disaster such as fire, vandalism, terrorism, system failure or natural disaster.

**PURPOSE:**

HPN is required by law to take reasonable steps to ensure accessibility to PHI and tax related data even in the event of a catastrophe; or at a least minimize the amount of time that PHI and tax related data is unavailable. No two disasters are the same and it is impossible to protect ourselves from every possible type of disaster; as such, the purpose of this policy is to implement the following steps which need to be followed independent of the type and scope of the disaster or catastrophe.

**DEFINITIONS:**


1. Security Officer (SO) - Responsible for administering the information security policies.
2. Host - A computer system that provides computer service for a number of users.
3. Server - A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.
4. Firewall - An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

**PROCEDURE:**

Disaster Recovery Plan

1. Assess damage, notify all appropriate personnel, assemble recovery teams, provide infrastructure (space, power, cooling, network, etc.), secure needed hardware and supplies, retrieve backup tape/s from safe or off-site storage, install operating systems on restored servers, restore applications and institutional data, and thoroughly test before going on-line.


**PROCEDURE (continued):**

 <p>Heritage Provider Network &amp; Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-018	Effective Date: 04/20/2005	Page - 2 -
	Authored by: David Pfafman	Date: 01/11/2006	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Disaster Recovery Plan			

## Interim Manual Procedures

1. Identify the procedure
2. Identify those with the knowledge, skill and ability to complete the procedure manually
3. Determine how long the process can be interrupted before proceeding manually
4. Develop detailed documentation on how the procedure will be performed
5. Determine how data is reintegrated once the IT-based system is restored
6. For the purpose of this policy we will focus on four specific scopes of disaster without specifying the type.
7. Single drive failure or data corruption, malicious software –Denial of Service attacks (DOS), hacks, viruses or worms. Typically these are always partial day outages at most.
8. Loss of a server or multiple servers. For this type of disaster expect 1-7 days with lingering effects in the case of a complete data center loss.
9. Complete data center loss or catastrophic loss of a site or multiple sites.
10. Loss of utilities and or telephone. With these different scopes there will be different levels continuation of business function.
11. In all of these scenarios the data backup is the key to any successful disaster recovery as such HPN and all entities are required to adhere to the HPN policy for data backup and retention (policy 14-011). As such each site is required to perform nightly backups on a two week rotation or cycle and keeping month-end tapes stored off-site for 1 year and year-end tapes stored off-site indefinitely. All other tapes should be stored in a fire-proof safe designed to protect media. (A normal fire-proof safe is designed to keep important papers from burning however tape media or CD/DVD media will be destroyed at temperatures much lower than the ignition point of paper.


PROCEDURE (continued):

 <p>Heritage Provider Network &amp; Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-018	Effective Date: 04/20/2005	Page - 3 -
	Authored by: David Pfafman	Date: 01/11/2006	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Disaster Recovery Plan			

12. Backups will be restored to a non-production server on a regular basis to verify the integrity of the backups. For consistency from site to site all locations will use Veritas Backup exec as their primary backup software.
13. Additionally all sites will have redundant LTO4 tape drives in place. Though other legacy drives can be used until in addition to the LTO4 drives.
14. Also relevant to all of these scenarios is the emergency notification list with their responsibilities. The emergency notification list is policy 14-019. In the event of a disaster local groups are required to notify at least one of the following: For data and operations disasters the HPN VP of MIS, for hardware or technical issues the HPN Director of IT for data security issues the HPN Information Security Officer (ISO).
15. The procedures for restoring PHI vary according to the scope of the disaster.
16. For single drive failure replacement of the defective drive is all that needs to be done because all mission critical servers are configured utilizing hardware RAID 5/10 technology. For data corruption and malicious software start trying to identify the scope of the corruption and/or isolate the compromised machine then contact the HPN ISO. Worst case scenario is that the data will have to be restored from the previous night's backup.
17. For single server failure, we will need to determine if the system is still under warranty. If so, get it fixed under warranty, and restore any lost data from tape. If it is not under warranty or there is going to be a delay in repair, the HPN Director of IT may know of other assets that can be reallocated on a temporary basis until the server can be repaired or replaced. For the loss of multiple servers we may need to move some or all of the data center functions to one of the other southern California data centers. In the case of a single or multiple server failure communications between the groups is critical as we can share assets between the groups in order to minimize downtime and loss to the company.
18. For complete data center loss or catastrophic site loss we still need to get mission critical systems up and functional as soon as possible. Because all of the southern California sites have remote sites that depend on the data at the primary site even though the site is down there are still people who need access to that data.

PROCEDURE (continued):

19. Additionally, as previously stated, we are legally required to maintain the accessibility of PHI as well as tax information. Since it is doubtful that any one data center will have the resources


 <p style="text-align: center;">Heritage Provider Network &amp; Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-018	Effective Date: 04/20/2005	Page - 4 -
	Authored by: David Pfafman	Date: 01/11/2006	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Disaster Recovery Plan			

to duplicate all of the functions of a remote data center it will be necessary to share the burden of the data center that is down across the remaining data centers. As an example if HPN Northridge is destroyed by an earthquake, RMG and HPN – finance would both be down. RMG EZ-CAP and other critical systems could be restored at DMG; HPN’s data warehouse could be moved to BFMC with the email and MAS-90 functions being covered by the Lancaster facility. Then we create a couple VPN’s and re-configure a few routers and workstations and at least the data is accessible again. Additionally, key personnel could be re-deployed to training rooms and conference rooms at the other facilities. Depending on the size of the disaster, one could expect to have very limited functionality in 2-3 days and be semi-functional within a week. Provisions will have to be made for critical phone numbers to be forwarded to functional phones. In the case of a regional disaster we need to be prepared to forward phones to a site out of the affected area. Sites also need to be prepared for the possibility of cell phone service being out as well. After major catastrophes such as 9-11, Katrina and the Northridge earthquake cell phone service was disrupted. Even in the best case the cell phone circuits would be overloaded and in a worst case they could be down for weeks.

20. Even though loss of electricity and/or phones is normally a short term occurrence it is potentially as damaging as an actual disaster. Our customers and patients may not be experiencing the same outages that we are and may lose faith in our ability to provide high quality service to them. Unfortunately there is little that can be done to fix the electricity or phones when they go out. Therefore HPN should plan ahead for outages of both. As such all mission critical servers, communications equipment, phone/PBX systems and workstations should have uninterruptible power supplies that will provide service for a minimum of 1 hour. Diesel generators should be installed at clinics if feasible. There will also be as much redundancy into our phones as possible. This can be done by using multiple carriers, having cell phones and single line phones to be used as backups or setting up VOIP or a PRI as a backup phone circuit. If one goes down, switch to the other.

PROCEDURE (continued):

21. Mission critical functions are those that are restored first in the event of a disaster. These applications are currently determined to be applications that contain critical data for continuity of business for UM, QI, clinical services, finance and the business office. These critical systems may change periodically as the organization’s needs change and will be reviewed.

 <p style="text-align: center;">Heritage Provider Network &amp; Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-018	Effective Date: 04/20/2005	Page - 5 -
	Authored by: David Pfafman	Date: 01/11/2006	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Disaster Recovery Plan			

Currently there are seven systems that are mission critical systems that have to be functional for us to provide service to patients:

- a. Phones
- b. EZ-CAP, including authorization and claims
- c. HDS applications
- d. NextGen
- e. Exchange Email
- f. Internet connectivity
- g. MAS 90

22. There are a lot of other ancillary programs that help us do a better job but we could still function without them, just not as well. As we add new systems and functionality it should be determined if that application is mission critical or ancillary in nature. A few examples of ancillary systems or non-Mission critical systems are listed below.

- a. Fax servers
- b. Claims Imaging
- c. EZ-Net
- d. EZ-EDI server
- e. Intranet

23. A log book should be kept in the safe and used to log all system outages (planned and unplanned), hardware failures, tape backup failures, data corruption and data loss to critical system. A copy of this log should also be kept electronically.

24. Everyone on the emergency notification and all MIS and IT staff should be trained as to where the disaster recovery plan is located and who to notify in case of a disaster. MIS and IT staff should know which non-mission critical systems and hardware need to be shut down to preserve battery life on the UPS's. All pertinent MIS and IT staff should know how to restore critical systems from tape using Backup exec. That way they are not putting a production system at risk while they are learning how to perform system restorations.

25. The disaster recovery plan should be distributed to everyone in the emergency notification list. A copy of the plan should be kept in plain sight in the server room and a copy should be kept in the safe just in case all of the other copies get destroyed.

26. Communications related to the systems availability will be provided through all methods available at the time. This communication will be made to both internal staff and to external providers, members, and to the public through the following channels: company website, provider portals, fax notifications, and/or telephone communications.



Heritage  
Provider Network  
&  
Affiliated Medical Groups

Program: Management Information Systems			
Policy No. 14-018	Effective Date: 04/20/2005		Page - 6 -
Authored by: David Pfafman	Date: 01/11/2006	Revised by: Scott Bae	Date: 02/02/2015
Approved by: Scott Bae	Date: 02/02/2015		

Title of Policy: Disaster Recovery Plan

27. The disaster recovery process will be tested periodically, at a minimum annually, to determine that the procedures ensure properly continuity of the critical systems. Some of the
28. The disaster recovery (contingency) plan will be revised when new critical systems are implemented as well as periodically to ensure that it is comprehensive for business continuity.