Arizona Computer Services, Inc. (ACS)
ACS' Contingency Plan Outline

ACS provides access to it's computers and software to accomplish medical billing for it's clients. Because Arizona Computer Services' (ACS') and it's client's data is extremely critical to each of their financial well-being and each of their operational needs, it is imperative that all anticipated operational interruptions are addressed. We have attempted to address these needs in the following pages.

DESCRIPTIONS

Services provided

ACS provides computer-related services to the medical community for the primary purpose of billing and receivables management. These include (but are not limited to):

- Providing and maintaining a stable hardware (computer) "platform"
- Providing and maintaining comprehensive medical billing software(s)
- Providing coding and billing expertise
- Providing hardware and software support staff
- Provide electronic claim submission/clearinghouse services (ECS)
- Providing appropriate and relevant training to client's staff
- Providing reports that meet the client's operational needs

PHYSICAL LOCATION

The main (Phoenix office) of ACS is located in a commercial office complex. There are two (2) entrances. Both entrances empty into public, well-lighted areas. The area is routinely patrolled by the Phoenix police department. Portions of the building (particularly those areas on entry and exit) are viewable from the exterior of the building, day or night, by both the police patrols and the private security guards that periodically patrol the office campus. The main door is simply labeled "ACS" as to not reveal the true nature of the business contained therein. The back door is only marked with the suite number. Access to the building is via coded access password and door locks. The alarm system, which incorporates infra-red motion sensors is monitored 24 hours a day, 365 days a year, and is linked to the local police and fire departments. There are 15-20 employees of Arizona Computer Services, Inc. (All offices)

The Casa Grande office of ACS is located in an office building in downtown Casa Grande. There are two (2) entrances. The main entrance empties onto a public well-lighted area. The rear door is always locked. The area is routinely patrolled by the Casa Grande police department. The office is only one block from the main police station.

EQUIPMENT

ACS' computer systems - ACS has two (2) mainframe-class computer systems at their site. Both are Digital Equipment VAX 4000 models. Access to the computer system(s) is limited to users that have a valid username and password. The VMS operating system under which the VAXs' operate (V6.2) also logs attempted break-ins and login failures. There are 2 levels of username/password security. The first username/password brings the user into the computer system the second set

logs the user into the appropriate practice with restrictions and privileges attendant with that userid.

A local PC LAN is also administered and maintained at the offices of ACS. This LAN is protected by a hardware "firewall" and also via layered username/password protection.

ACS technical support staff is available to our clients (via pagers) 24 hours/day.

Communication systems – ACS provides several mechanisms by which connection to the VAX computer systems are possible; Dial-up, leased-line, and Internet.

Dial-up service – Connection to the VAX is possible from either a "dumb terminal" (i.e., Digital VT-520, Wyse-85, etc.) or from a personal computer (IBM-style PC or Apple) utilizing a terminal emulation package. The dial-up lines feed into an array of modems that range in potential speeds from 9600 baud to 56K baud). A group of phone numbers are assigned to clients using the dial-up option in the event that the "main number" assigned to them is busy or out of service. The modems are connected to a terminal server utilizing DECNET protocol via a serial connection. The servers are connected to both the VAX computers and ACS' LAN via an Ethernet connection.

Leased line service - Connection to the VAX is possible from either a "dumb terminal" (i.e., Digital VT-520, Wyse-85, etc.) or from a personal computer (IBM-style PC or Apple) utilizing a terminal emulation package. The leased lines feed into either muliplexer (ACS utilizes primarily Datarace and MultiTech multiplexers; from 4-32 channel capacities) from a T-1 channel bank or direct connection. The multiplexers are connected to a terminal server utilizing DECNET protocol via a serial connection. The servers are connected to both the VAX computers and ACS' LAN via an Ethernet connection.

Internet connection – Connection to the VAX (via the Internet) is accomplished with a personal computer, laptop, etc (Windows, Apple, Linux, etc) utilizing an Internet browser (Explorer, Navigator, Mozilla, etc) running an Active-X component available at our website, http://www.acsmedicalbilling.com. A remote client connects to the VAX computer systems through a their ISP to ACS' website link, which refers to a Windows 2000 Professional Server running WebConnect by Ericom encrypted with SSL and connected to a DMZ port on an Instagate EX firewall appliance. Traffic is passed locally to a TCP-enabled P4000 - series Emulex terminal server, which translates the signal to Decnet and passes it on to the VAX systems. The firewall and network status is reviewed by the system operator.

Internet connection – Connection to the VAX (via the Internet) is accomplished with a personal computer (IBM-style PC or Apple) utilizing a terminal emulation package or via an internet browser with a TCP/IP emulation package. A remote client can connect to the VAX computer systems via the Internet. TCP/IP protocol is utilized over a DSL line to connect to ACS' VAX computer system through a hardware/software firewall. Connection to the terminal emulator embedded in the website requires that the connection be 128-bit encrypted. The firewall and network status is reviewed by the system operator.

CARE/DM billing system - The Internet connections feed to a terminal server via an Ethernet connection and to the VAX computers via the Ethernet connection.
ProData billing system – The ACS website www.acsmedicalbilling.com transfers the client directly to the ProData website www.prodata.com where the client connects to the Intel-operated/maintained site housing ProData's programs and the client's data. The connection requires 128-bit encryption.

Backups

Clients running the CARE/DM billing system: Backups of client data are performed each time a client (or ACS on their behalf) submits a "daily close" from within the billing software. Total system backups are also routinely scheduled.
The data is backed up to either a 4mm DAT tape drive or a 1/4" cartridge tape and the media is stored, on-site, within a magnetic media rated fireproof safe. Monthly, a copy of these tapes are taken home by the operations supervisor for additional protection. ACS has also contracted with Caremaster, Inc. Of Dallas, TX to be an emergency "hot site" in the event of a catastrophic hardware failure (i.e., Total destruction of ACS' facilities and computer systems).
Clients running the Prodata billing system: The data is maintained at a secured Internet site (ASP model) on fault- tolerant systems utilizing RAIDS and/or disk-shadowing as methods of data protection along with routine tape backups of all client data. Power protection at the Intel-administered site is provided through battery backup AND diesel generators (for prolonged power outages).
Virus protection within the ProData system is accomplished through the Intel-operated/maintained (ASP model) sites. Intel takes great pains to protect the systems which they are responsible for.

Access controls - Access to ACS' computer systems is via layered username and/or password protection. All transmissions via Internet connections are using 128-bit encryption. A hardware "firewall" is employed to eliminate break-ins from the Internet. Physical access to the computers at ACS is limited to employees and escorted visitors.

Password protocols - (CARE/DM system only) ACS has three (3) technical support personnel that are qualified to alter the system-wide username/password authorization files. It is recommended that the client work with the technical support staff to assure adequate protection.

At the client's option, ACS can:
- Set password minimum length
- Set password expiration times (i.e., 60 days)
- Limit access times/days
- Automatically "lock up" a username that has had "x" login failures.

At the individual userid (within a client/practice) level, ACS can:
- Limit individual userids to "lock out" access to individual menu selection(s).
- Log (journal) login and logout times.

ACS website - The ACS website (www.acsmedicalbilling.com) is built to automatically utilize 128-bit encryption wherever it is necessary. Access to Protected Health Information (as defined in the HIPAA regulations) through the various "links" in the ACS webpage are the responsibility of the companies and/or agencies which are "linked to". If ACS encounters a linked website that is NOT conforming to the security standards as defined under HIPAA regulations, ACS will immediately remove the link to the offending site from the ACS website.

Potential failures and their contingency plans/procedures

The funding for all failures other than those described under the heading of total system meltdown are accomplished out of ACS' operation budget. Major failures would require insurance funding.

Connection failures

Phone number assigned to dial-up user is busy or not operational

1. User should attempt connection using the alternate phone numbers assigned to the user.
2. If all alternate numbers are busy or not operational, user should notify ACS tech support. Tech support staff will research and resolve the problem.

EXPERIENCE: Due to the sheer number of modems employed at ACS (approximately 20), we have experienced this routinely. The average response time is 2-20 minutes.

All (or most) of the dial-up numbers are not operational

In the event that all/most of the dial-up lines are "down" due to a problem from ACS' current telecommunication provider (currently Qwest) and/or T-1 network carrier problem, ACS is at the mercy of those carriers. ACS will report the outage to the appropriate carrier and track the progress of the repair.

EXPERIENCE: ACS has experienced 4 failures of T-1 services in the last 5 years. We have switched T-1 carriers as a result. Average time to repair has been 6 hours.

Leased line is not operational

1. The user should immediately report the situation to ACS technical support staff.
2. ACS technical staff will test the individual client's equipment to verify that the problem rests in the communication line.
3. The leased line carrier (typically Qwest) will be notified of the failure. The leased lines carry a higher priority with the carrier and dispatch of a repair technician is usually accomplished within 4 hours of the incident being reported.
4. ACS technical staff will track the progress of the repair and notify the effected client when repairs are accomplished.

EXPERIENCE: ACS experiences leased line failure approximately 3 times/year. Average time to repair has been 4 hours.

Modem is not operational

1. The client should notify ACS technical support staff of the problem.
2. ACS technical support staff will verify that the modem is not operational.

3. As ACS maintains several "standby" modems, the equipment can be replaced immediately. (If the modem at the client's location is found to be "dead", ACS will deliver and install a replacement [usually within 4 hours of the notification])
4. If no replacement is found in ACS' inventory, replacement equipment can be ordered through a local vendor. Delivery from the vendor is typically from 4 hours (if equipment is in vendor's inventory) to 48 hours (If it needs to be ordered and "overnighted" to the vendor)

EXPERIENCE: ACS has experienced multiple failures of modems (approximately 1/month) and has typically responded to all of these instances within 4 hours. Average time to correct a modem (at ACS' site) is 15 minutes.

Multiplexer is not operational.

1. The client should notify ACS technical support staff of the problem
2. ACS technical support staff will verify that the multiplexer is not operational.
3. ACS strives to maintain several standby multiplexers, the equipment can usually be replaced immediately. (If the multiplexer at the client's location is found to be "dead", ACS will deliver and install a replacement [usually within 4 hours of the notification])
4. If no replacement is found in ACS' inventory, replacement equipment can be ordered through a local vendor. Delivery from the vendor is typically from 4 hours (if equipment is in vendor's inventory) to 48 hours (If it needs to be ordered and "overnighted" to the vendor)

EXPERIENCE: ACS has experienced multiple failures of multiplexers (Less than 1/month) and has typically responded to all of these instances within 4 hours. Average time to correct a multiplexer failure (at ACS' site) is 15 minutes.

Terminal server is not operational

1. The client should contact ACS technical support. This failure will "knock down" many (up to 32) terminal connections.
2. ACS technical support staff will verify that the terminal server is not operational.
3. As ACS maintains an inventory of spare "boards" for terminal servers, most server problems can be repaired within 1 hour.
4. If no replacement is found in ACS' inventory, replacement equipment can be ordered through a local vendor. Delivery from the vendor is typically from 4 hours (if equipment is in vendor's inventory) to 48 hours (If it needs to be ordered and "overnighted" to the vendor)

Internet failure

Connection to ACS via the Internet connection (described above) is vulnerable to failure at either the client site (Their Internet service provider [ISP] fails.) or ACS' ISP fails. As ACS moves towards more Internet connections (as opposed to dial-up and leased line services traditionally employed by ACS) and the planned implementation of Electronic medical records (EMR) software, it is planned that the failure of ACS's Internet connection will be protected in the following manner:

1. A firewall with dual internet connections with an automatic fail-over will be purchased.
2. A second (redundant) firewall will be purchased.
    a. Should the (anticipated) T-1 Internet connection fail, the firewall will automatically connect through internal fail-over mechanism to a stand-by DSL or cable (lower speed) connection..
    b. Failure would then be possible only if BOTH the T-1 AND the DSL/cable ISP be unavailable. This possibility is calculated to be extremely remote. Limited dial-up service would be available in the event of a total Internet failure. As EMR is implemented, a more detailed plan will be available.

Computer component failures

Tape/tape device failures

ACS utilizes at least 2 tape drives to accomplish the backup routines (described elsewhere).

1. A **4mm DAT** drive is used to do the daily backups. This drive is a magazine-fed drive holding 10 tapes, each capable of (at least) 1.2GB of data. 2-4 tapes are typically required to accomplish a daily backup. The 4mm DAT tapes (as is true of all magnetic media) deteriorate with usage and handling. Tapes are "retired" and consequently destroyed in such a manner as to make all data that may remain on the tape completely irretrievable.
    a. In the event of a failure of the 4mm DAT device, a replacement will be ordered. Replacement time is typically 48 hours. Since the backup routine is not critical to the ongoing operation of the client's billing process and a second tape drive can be "pressed into emergency service" as an alternate, a 48-hour repair/replacement time is acceptable. No spares are maintained within the ACS inventory.

2. A **¼" QIC (Quarter-inch cartridge) tape drive** is used to do the month-end backups (fully described elsewhere in ACS' HIPAA Compliance Manual). This device is a single cartridge device. Each QIC cartridge holds approximately 2GB of client data. Approximately 4-5 cartridges are required to accomplish a typical month-end backup.
    a. In the event of a failure of the ¼" QIC (Quarter-inch cartridge) tape drive a replacement will be ordered. Replacement time is typically 48 hours. Since the backup routine is not critical to the ongoing operation of the client's billing process and a second tape drive can be "pressed into emergency service" as an alternate, a 48-hour repair/replacement time is acceptable. One spare is maintained within the ACS inventory.

Should the Restore function fail during attempted recovery of client data, ACS technical support staff should immediately test the tape device that the failing tape was written on to determine if the inability to retrieve data is due to media failure (defective tape) or device failure (bad tape drive).

1. If the media (tape is found to be corrupt, ACS tech support staff should either label the tape as "NOT USABLE" or destroy the tape in such a manner as to render the data irretrievable.
2. If the tape drive has failed/is failing then ACS support staff should proceed as outlined above under "Tape/tape device failures" of this document.

Tape drives have failed at ACS at the rate of approximately 2/year. They were repaired or replaced. During the absence of the failed equipment, operational procedures (as described above) were followed. There was no interruption of services to ACS' clients during these failures.

Disk failure

The VAX system is currently supporting 6 disk drives clustered via a DSSI connection. Client data typically resides on a single disk drive – not scattered across multiple drives. In the event of a disk failure, ACS tech support has several options:

1. **The data lost on the failed disk is small** (compared to the remaining free blocks on the remaining disk drives) ACS attempts to maintain a minimum of 100,000 clusters (of 512 bytes) of open space on each drive. For most clients, this empty space is enough to be able to "squeeze them on to" in the event that "their" disk fails. If the remaining drives contain enough free space to accommodate the recovery of the failed disk then ACS technical support staff will:
    a. Restore the data from the backup tapes to the remaining disk drives.
    b. Locate and order a replacement disk drive from a hardware vendor.

c. When the replacement is installed, the client data will once again be "load balanced" on the disk drives.
d. Mean time to correct this failure is estimated at 3-12 hours-

2. **The data lost on the failed disk cannot be fit on the remaining free space.**
   a. Locate and order a replacement disk drive.
   b. When the replacement disk is installed, the client data will be restored from the backups save sets.
   c. The mean time to correct this failure is estimated to be 24-72 hours. (this time is primarily dependent upon the time taken in locating and shipping a replacement disk drive)

ACS has experienced a disk failure 3 times in 20 years. A complete recovery was accomplished in all cases. (Recovery of data from the client's prior backup tapes)

Printer failure

Main printers (at ACS) - ACS employs two (2) high volume, medium speed, laser printers. The decision to acquire two printers rather than a single, high-speed laser printer was based on redundancy. One is a Konica model 7040 (40ppm capacity). The other is a Konica model 7033 (33ppm capacity). Each is capable of handling the entire print cycle of a month end run for all clients. Therefore, if either printer fails the remaining operational printer can be used to "shoulder" the entire load. These printers are also covered under a maintenance agreement with Hughes-Calihan (copies available upon request).
EXPERIENCE: ACS has experienced failures of these printers at crucial (month-end) times. No loss of service or capacity was experienced by our clients. ACS has always had plenty of additional printing capacity in other on-site printers.

Secondary printers (at ACS) - ACS employs several printers (lasers, ink-jets, impact, and dot matrix)to accommodate special forms (pin-feed, insurance forms, labels, etc.). Failure of any of these devices in non-critical as the print jobs can be re-routed, by ACS technical support staff, to other operational printers.

Printers (at client site) – ACS maintains a small inventory of impact and laser printers. These devices (if not in ACS' inventory) are available quickly from a local hardware vendor. Most items are available for immediate pickup. During the "down-time", the client can opt to have ACS print and deliver the client's reports or the jobs can be re-routed to a different printer at the client site.

Terminal failure

There are approximately 200 terminals connected to the CARE/DM software and the VAX computers. ACS maintains an inventory of several stand-by terminals to replace failed terminals.
EXPERIENCE: Due to the sheer volume of terminals, ACS experiences failure of terminals at the rate of approximately 2/month. Average time to replace a failed terminal is 4 business hours.

Computer failure

ACS uses two (2) VAX 4000 computers in the deployment of the CARE/DM billing system. Each system is currently carrying less than 40% of it's capacity during a typical day of processing. If either system should fail, the remaining system could be used to accommodate ALL of the processing. (Redundant system model). This re-routing of connections could be accomplished by ACS technical staff in less than 2 hours. The failed system could then be repaired by Compaq (or similar hardware repair technicians). Mean time to repair a failed system is estimated to be 7 days. An alternative to repair would be to purchase a used system from a local hardware vendor. Replacement time is estimated to be 4 days. ACS technical support staff will weigh it's options/benefits and take the appropriate action.
EXPERIENCE: ACS has experienced no failures of a computer system in over 7 years.

Personal computers (PC's) – ACS uses PC's peripherally to it's operation. (upload/download of client data, e-mail, voice mail, etc) The failures of PC's and the Local Area Network (LAN) to which the PC's are connected have no significant impact on the billing process or ACS' operational status.
EXPERIENCE: ACS has encountered disk failures, viruses, and system failures on their PC's. PC systems and or disks were replaced. Viruses were either eliminated or the operating systems rebuilt. No resultant data loss or corruption of client data was experienced. The Local Area Network (LAN) employed by ACS has also experienced multiple failures of all or part of the LAN. No resultant data loss or corruption of client data was experienced.

Software failures

Operating system failures – VMS V6.2 is a mature and ultra-stable operating system. MTBF (mean time between failures) of the VMS operating system is expressed in YEARS rather than the typical days associated with a Windows-based system. VMS was originally designed by Digital Computer Corp. in 1972. The VMS operating system has been in use at ACS since 1982. During that time, NO FAILURES of the operating system have been recorded in the last 10 years. No contingency plan is in place for this failure. A re-build of the operating system could be accomplished by ACS technical support staff in approximately 8 hours. Distribution tapes of the VMS V6.2 operating system are maintained at ACS.
EXPERIENCE: ACS has experienced NO failures of the VMS operating system in 7 years.

Billing software failures – As of September 1, 2002, ACS has taken on the national support of the CARE/DM product. ACS has used the CARE/DM medical billing software since 1982. As of 1996 there are no known serious "bugs" in the software. ACS has historically been able to either fix or "work around" all reported problems within the software since 1999. ACS does have access to the CARE/DM source code (since 1999) and maintains 2 programmers as part of their technical support staff.
EXPERIENCE: Since 1999, when ACS obtained access to the CARE/DM source code, no major software failures have been encountered. The minor failures that were reported have been responded to within 24 hours. No data loss or corruption of client data has been reported.

Backup (save or recovery) failure - Failure of backup and/or recovery would be associated with either a media failure or a tape drive failure. Each of those potentialities is fully discussed in this document under Computer Component Failures; Tape/Tape Drive Failures
EXPERIENCE: Only one recovery failure was noted in the last 7 years. In that instance, one day's activity was lost for the client..

Virus protection – There is no need for virus protection on the VAX as there are no known viruses currently being written for the VMS operating system.
EXPERIENCE: No virus has ever been detected on the VAX system.

Disasters, Natural / Caused

Disasters of all types could ultimately lead in multiple failures previously mentioned in this document. Regardless of it's cause (e.g. flood, water damage, sabotage, etc.), we would handle single device failures as outlined above. The worst failures would result in all (or a considerable number of) the above described equipment failures. Usually, this could also involve destruction of not only the computer equipment, but the ACS facilities as well.

ACS maintains insurance coverage on the equipment housed at ACS in the amount of $1 million per occurrence, $2 million aggregate through Zurich American Insurance. These funds would be the resource by which a large-scale rebuild of ACS would be financed.

Total system "meltdown" – In the event that not only is the computer system rendered inoperable, but the facilities of ACS are destroyed, an entire company re-build would have to be accomplished. The following steps would be followed:

1. Notify ACS clients of the failure.
   a. Set up a voice-mail/announcement on the ACS support telephone number.
   b. ACS technical support staff will also notify ACS clients by telephone.
   c. ACS technical support will e-mail clients (where ACS has been provided e-mail addresses)
2. Rebuild facilities.
   a. A location within the same office complex is preferable. This would facilitate and simplify the re-wiring of the phone and data communication systems. A minimum of 200 square feet of space is required to rebuild the "computer room". This would require approximately 24-48 hours to accomplish.
3. Set up a "hot-site". Using a "hot-site" would allow ACS clients the ability to access their client data (from the last "good backup") via an Internet connection. This would require a PC and an ISP connection at the client's site.
   a. There are two (2) service bureaus that utilize the CARE/DM software that ACS has mutually contracted with to provide "hot-site" services should the other's facilities be rendered unusable.
      Caremaster, Inc. Of Dallas, Texas
      ProData Payroll Services, Inc. of Burlington, Iowa
   b. One (or both) of these sites would be provided with the most current version os client backup tapes to be restored on their computer system(s). Connection to these "hot-site" system(s) would be available via an Internet connection. Approximate time to make client data available at the "hot-site(s)" is 24 hours.
4. Acquire replacement equipment.
   a. Computers: Replacement time estimate: 5 days
      Software replacement:
      Operating system-VMS V6.2. Replacement from off-site backup- 4 hours
      CARE/DM source and object libraries. Replacement from off-site backup - 4 hours
   b. Communication equipment replacement.
      General telecommunication services - 4 days to re-establish services.
      T-1 channel bank - 5 days to replace
      InstaGate firewall - 3 days to replace
      Modems, multiplexers, bridges, etc. - Replacement from misc vendors...5 days replacement time.
   c. Tools, wire, misc. replacements would be from various vendors, most with a replacement time of 24-48 hours.
5. Re-establish connections. Approximately 1 day would be required to re-wire and reconnect the replacement equipment.
6. Rebuild system and VMS operating systems. Approximately 1 day would be required to rebuild the computers and their operating systems.
7. Restore client data from most current backup available. Rebuilding client data from tape archives will require 6-36 hours.
8. Notify clients of ACS' return to normal operation.
9. Where applicable, retrieve and restore data from "hot-sites" onto the rebuilt systems.

Most of these activities can be run concurrently by different ACS technical support staff people. It is estimated that the ACS operations would be "down" for 14 days in the case of a "total system meltdown" failure. The maximum data loss (if the fireproof media safe at ACS and it's contents are destroyed) would be 7 days.

Power failure – ACS uses a 2.4KVA battery backup/power isolation unit to guard against momentary loss of power. During a power failure, the battery backup of the unit "kicks in" and provides approximately 30 minutes of power to the VAX CPU and the operator's console. The operator can perform an orderly shutdown of the system. No data loss occurs under the VMS operating system as

a result of a power loss. NO EMERGENCY BATTERY POWER IS SUPPLIED TO THE COMMUNICATION EQUIPMENT. Therefore, during a power outage, the client connection is lost, but the data remains intact. When the power is restored by the utility company, it takes about 12 minutes to re-boot the VAX systems.
EXPERIENCE: Approximately 2-3 times per year, particularly during the monsoon season in Arizona, ACS experiences power outages. No data loss or corruption of client data has ever been experienced in 7 years.

ACS Employee "failure" – ACS employs three (3) individuals in the capacity of technical support. Each of those individuals is capable of handling ANY of the failures described herein.
EXPERIENCE: In the technical support staff, ACS has not had turnover or employee failure in the last 7 years.

Economic "failure" of ACS - In the event of ACS' insolvency the operations of ACS would cease. Clients are encouraged to periodically request that a backup tape or CD of their data be delivered to the client and stored at the client's site. A small tape charge may apply (approximately $15 per tape)
EXPERIENCE: ACS has been in operation since 1970. Economic "failures" have not been experienced since 1970 nor are any economic "failures" anticipated.

SUMMARY

As ACS is in the business of "renting" it's hardware, software, technical expertise, etc., it is imperative that we have in place and periodically test our contingency plans. Because of ACS' 20+ years of experience with the hardware and software which we have in place, we have experienced and responded to all of the above failures (except "total system "meltdown", employee "failure", and economic "failure"). We are confident in our continued ability to provide high reliability and availability of our services.

These operational descriptions should be placed within each client's own contingency plan documents as required by HIPAA regulations.

C:\hipaa\Documents\ACS-Contingency Plan.wpd Revised: October 2, 2003