

Attachment M.1.c  
WellCare IT Disaster Recovery Plan



# Information Technology

---

## Disaster Recovery Plan

**COMPREHENSIVE HEALTH MANAGEMENT, INC.**

**NOTICE**

Data Classification: Confidential, Unpublished Property of WellCare Health Plans, Inc. – Do Not Duplicate or Distribute.  
Use and Distribution Limited Solely to Authorized Personnel

**Revision History**

<b>Revision</b>	<b>Release Date</b>	<b>Author</b>	<b>Changes in progress</b>
1.0	02/10/2010	W. Greg Brooks	Initial Release
1.1	04/27/11	W. Greg Brooks	Updated key contacts information.

**Approvals**

<b>Name</b>	<b>Title</b>	<b>Signature</b>	<b>Date</b>
W. Greg Brooks	EPC IT Representative	see embedded .pdf below	4/27/11
Paul Kohler	I.T. VP / Infrastructure	see embedded .pdf below	4/28/11



H:\My Documents\  
STATE\EPC\2011\_EPI

**NOTICE**

Data Classification: Confidential, Unpublished Property of WellCare Health Plans, Inc. – Do Not Duplicate or Distribute.  
Use and Distribution Limited Solely to Authorized Personnel

**Table of Contents**

---

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>2</b>	<b>SCOPE .....</b>	<b>4</b>
<b>3</b>	<b>I.T. DISASTER PREPAREDNESS PROCEDURES.....</b>	<b>4</b>
3.1	IT DR Event Preparation Time-line .....	4
3.2	Event Alert Procedures .....	5
3.2.1	Event Alert Procedure .....	5
3.2.2	DR Vendor (SunGard) Alert Procedure.....	6
3.2.3	Prepare DR Tape Backup Media for Shipment Procedure .....	6
3.2.4	Secure Travel / Lodging for IT Away Team Procedure.....	7
3.3	Event Preparedness Activation Milestone Procedures .....	8
3.3.1	Event Preparedness Activation Notification Procedure .....	8
3.3.2	Recovery Media Emergency Shipment Procedure .....	9
3.3.3	I.T. DR Away Team Emergency Travel Procedure .....	10
3.4	Event Watch Milestone Procedures .....	10
3.4.1	Event Watch Notification Procedure .....	10
3.4.2	Establish IT DR Situation Room Procedure .....	11
3.4.3	Disaster Recovery Declaration Decision Procedure .....	11
3.4.4	Disaster Recovery Declaration w/ Remote Recovery Vendor Procedure.....	12
3.4.5	Remote DR Network Initiation.....	12
3.4.6	Execute Remote Data Center Recovery Procedure .....	12
3.4.7	Recovery Point Objective (RPO) Synchronization Procedure .....	13
3.5	Event Warning Milestone Procedures.....	13
3.5.1	Event Warning Notification Procedure .....	13
<b>4</b>	<b>I.T. DISASTER RECOVERY PROCEDURES .....</b>	<b>15</b>
4.1	Post-Disaster Corporate Damage Assessment Procedure .....	15
4.2	Critical Applications Recovery Sequence .....	16
4.2.1	DR Phase I Recovery Priority Matrix.....	16
4.2.2	DR Phase II Recovery Priority Matrix.....	17
4.2.3	DR Phase III Recovery Priority Matrix.....	18
4.3	Remote Data Center Recovery Procedures.....	19
4.3.1	Execute DR Network Recovery Procedures .....	19
4.3.2	Configure DR Host Servers.....	19
4.3.3	Configure / Allocate Storage .....	19
4.3.4	Execute Citrix Recovery Procedures .....	20
4.3.5	Execute Exchange Recovery Procedures.....	20
4.3.6	Execute Veritas Recovery Procedures .....	21
4.3.7	Restore Critical System Back-up Images.....	21
4.3.8	Recover Critical Applications .....	21
<b>5</b>	<b>APPENDIX.....</b>	<b>23</b>
5.1	SunGard Disaster Declaration Authority List.....	23
5.2	IT DR Incident Management Team List .....	23
5.3	IT DR Team List.....	24

**NOTICE**

## 1 INTRODUCTION

The Information Technology Disaster Recovery Plan (IT DRP) establishes the WellCare Information Technology (IT) data center remote recovery procedure. The plan outlines the procedures to be executed in the event the Corporate Data Center is non-functional and information or telecommunications processing capabilities are not available.

WellCare has a contract with SunGard Recovery Services, Inc. to provide remote recovery of the WellCare corporate data center and critical business systems. SunGard is a leading provider and nationally recognized provider of information availability solutions.

The plan includes procedures to restore IT managed services and information processing infrastructure. Additionally, this document contains procedures to manage activities in preparation of a pre-announced event that will have significant impact to the Corporate Data Center and affecting information or telecommunications processing. The plan addresses events including, but not limited to the following: extended power outage, extended network outage (LAN / WAN), severe data corruption, security threats, environmental disruptions, and localized disasters.

The IT DRP is activated per the direction and authority of the WellCare Corporate Emergency Preparedness Committee (EPC) in cooperation with the WellCare Information Technology (I.T.) CIO.

The disaster preparation procedures are executed in its entirety or parts depending on the available amount of time leading up to the event. A preparation timeline is provided to show the various steps to be taken prior to the event. Each procedure includes a set of actions, as well as the criteria, person, and timing to execute the actions. Also, included in the preparation plan are the communication, notification, and logistical procedures. The disaster preparation procedures are contained in Section 2 of this document.

The disaster recovery procedures (contained in Section 3) are executed after the event to restore IT services and information processing infrastructure at a remote data center if the Corporate Data Center is not available. The same steps and procedures are followed regardless of the type of event or if preparation procedures were executed. The recovery procedures identify restoration decision points, criteria, actions, contacts, and responsible individuals. These procedures are to be executed by qualified personnel with experience in the respective technology. Detailed restoration procedures specific to each technology are not contained in this document but are stored at the remote data facility.

The recovery sequence is divided into three phases. Business requirements are taken into consideration for the restoration of critical business applications.

The DR Phase I recovery efforts focus on establishing the technology infrastructure and framework from a network, server and storage perspective, and integration services (ESB), as well as recovering critical customer facing, vendor facing and corporate ERP systems.

The DR Phase II recovery efforts focus on establishing the channel services (EDI), batch processing services (AutoSys). Additional operational support systems are also recovered during the Phase II Remote Data Center Recovery Process.



Event Phase	Time-line	Activities	Owner
Event Preparedness Alert	T0 (-) 120 to 72 hours	<ol style="list-style-type: none"> <li>1. Issue Event Preparedness Alert</li> <li>2. Alert DR Vendor (SunGard)</li> <li>3. Identify / Secure Critical Tape Backup</li> <li>4. Secure Travel / Lodging</li> </ol>	<ol style="list-style-type: none"> <li>1. IT DR Project Mgr</li> <li>2. IT DR Project Mgr</li> <li>3. IT Infrastructure</li> <li>4. IT DR Project Mgr</li> </ol>
Event Preparedness Plan Activation	T0 (-) 60 hours	<ol style="list-style-type: none"> <li>1. Issue Event Preparedness Activation Notification</li> <li>2. Ship Recovery Media</li> <li>3. I.T. DR Team Travels to Remote Recovery Site</li> </ol>	<ol style="list-style-type: none"> <li>1. IT DR Project Mgr</li> <li>2. IT Infrastructure</li> <li>3. IT Away Team</li> </ol>
Event Watch  (SunGard Disaster Declaration)	T0 (-) 48 hours	<ol style="list-style-type: none"> <li>1. Issue Event Watch</li> <li>2. Declare Disaster w/ DR Vendor (SunGard)</li> <li>3. Start Phase I remote recovery</li> <li>4. Establish Emergency Operating Mode Strategy (workforce Strategy)</li> </ol>	<ol style="list-style-type: none"> <li>1. IT DR Project Mgr</li> <li>2. Corporate Executive</li> <li>3. IT Away Team</li> <li>4. IT Leadership</li> </ol>
Event Warning	T0 (-) 24 hours	<ol style="list-style-type: none"> <li>1. Issue Event Warning</li> <li>2. Activate Emergency Mode of Operations</li> </ol>	<ol style="list-style-type: none"> <li>1. IT DR Project Manager</li> <li>2. IT Leadership</li> </ol>
Event Impact	T0	<ol style="list-style-type: none"> <li>1. Monitor Event</li> <li>2. Update Communications</li> </ol>	<ol style="list-style-type: none"> <li>1. IT DR Project Mgr</li> <li>2. IT DR Project Mgr</li> </ol>
DR Cut-over Decision	T0 (+) 16 hours	<ol style="list-style-type: none"> <li>1. EPC decision to cut-over to remote DR Data Center</li> <li>2. If 'no' continue operations at corporate campus</li> <li>3. If 'yes', begin corporate data center shutdown and cut-over to remote facility</li> <li>4. Execute IT Emergency Mode of Operations</li> </ol>	<ol style="list-style-type: none"> <li>1. EPC / IT CIO</li> <li>2. N/A</li> <li>3. IT DR Response Team</li> <li>4. IT All</li> </ol>

**Table 1: Disaster Event Phases**

### 3.2 Event Alert Procedures

The following procedures are initiated at the discretion of the IT DR Project Manager based on event information from a recognized, official source; i.e., FEMA, National Weather Center, etc.

#### 3.2.1 Event Alert Procedure

**Criteria:** An event alert is issued at the discretion of the IT DR Project manager, when an official source issues formal or informal notification of a pending event.

**Actor:** IT DR Project Manager

**Timing:** 120 hours to 72 hours in advance of projected event impact

**Action:** **Issue Event Alert to IT Leadership and IT Away Team**

1. Via email, the IT DR Project Manager will notify 'All IT Managers' as identified in the Company active directory that an Event Alert has been issued.
2. Via email, the IT DR Project Mgr. will notify identified IT DR Team members (refer to the appendix of this document for a current listing of IT Team Members).
3. Via Outlook Calendar, establish a once daily recurring Event Alert update meeting. Use the below DR conference number for telephone attendees:  
Toll Free Dial In Number: (877)402-9753  
Int'l Access/Caller Paid Dial In Number: (636)651-3141  
ACCESS CODE: 1008220 HOST PASSWORD: 4210

### 3.2.2 DR Vendor (SunGard) Alert Procedure

**Criteria:** A DR Vendor alert is issued immediately following the issuance of the Event Alert.

**Actor:** DR Project Manager

**Timing:** 120 hours to 72 hours in advance of projected event impact

**Action:** Issue DR Vendor Alert:

1. Via telephone, the IT DR Project Manager will notify the current DR Vendor (currently SunGard) that WellCare Comprehensive Health Plans, Inc. has issued an Event Alert for the corporate campus.  
Call SunGard at the below number using the identified company name and customer ID;  
SunGard Phone: (866) 722-1313  
Customer Name: Comprehensive Health Management, Inc.  
CARES Customer Id: 32060
2. Referencing the WellCare DR contract w/ SunGard, identify the schedule of equipment and resources that are placed on alert. The contract is maintained by the IT Budget and Finance Department.

### 3.2.3 Prepare DR Tape Backup Media for Shipment Procedure

**Criteria:** Critical Backup media is identified and prepared for emergency shipment when WellCare issues an Event Alert for the corporate campus.

**Actor:** I.T. Infrastructure / IT DR Project Manager

**Timing:** 120 hours to 72 hours in advance of projected event impact

**Action:** Identify / Prepare Tape Backup Media for Shipment:

1. Identify DR Recovery Backup Media (IT Infrastructure)
  - a. Using the corporate backup software (Veritas NetBackup), identify all physical tape IDs for the last three (3) full critical and production backups.
  - b. Collect and prep all identified tapes that have not been forwarded to the tape archive.
  - c. Create list of critical backup media that is located at the tape vendor's location.
2. Alert Tape Vendor of Pending Tape Shipment  
Archive Corporation Phone #: (813) 874-1577  
Archive Corporation Address: 6914 Asphalt Rd, Tampa Fl. 33614
3. SunGard Tape Receiving Address:  
SunGard Address: 777 Central Boulevard, Carlstadt, NJ 07072

SunGard Contact: Orlando Rodriguez  
SunGard Phone #: 201-729-2389

### 3.2.4 Secure Travel / Lodging for IT Away Team Procedure

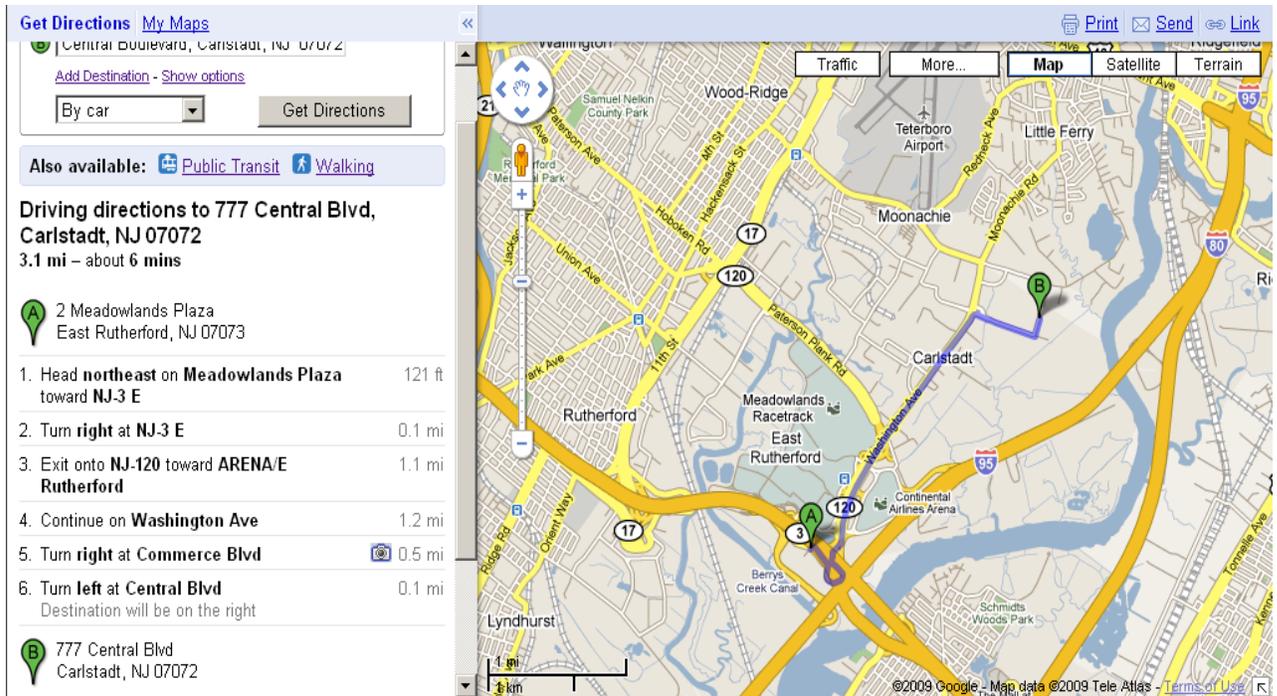
**Criteria:** I.T. Away Team travel and lodging is secured per the authority of the EPC and CIO. The IT DR Project Manager requests the activity once an Event Alert is issued.

**Actor:** I.T. Away Team / IT DR Project Manager

**Timing:** 120 hours to 72 hours in advance of projected event impact

**Action:** Secure Travel / Lodging for I.T. Away Team:

1. Minimum Away Team Requirements
  - (1) Backup Engineer
  - (1) Server Engineer
2. Obtain Corporate MasterCard from I.T. Infrastructure Director. The decision as to when to book the travel and lodging is based on the risk and threat of the impending event. As such, while the travel and lodging should be immediately acted on from an availability perspective, prior to booking, formal authority must be obtained from the CIO or delegate.
3. Away Team members need to be registered w/ the current corporate travel service (see IT Administrators). Refer to Appendix 5.3.
4. Preferred Hotel: Sheraton Meadowlands Hotel and Conference Center; Carlstadt, New Jersey
  - Sheraton: (201) – 896-0500
  - Address: 2 Meadowland Plaza, East Rutherford, NJ 07073
5. SunGard Physical Address:
  - SunGard Address: 777 Central Boulevard, Carlstadt, NJ 07072
  - SunGard Contact: Orlando Rodriguez
  - SunGard Phone #: 201-729-2389



**Figure 2: Remote Facility Directions / Map**

### 3.3 Event Preparedness Activation Milestone Procedures

Event Preparedness Activation procedures are activated as early as 60 hours prior to predicted event impact.

The following procedures are initiated per the authority of the Corporate Emergency Preparedness Committee and the Information Technology Chief Information Officer (CIO) or delegate(s).

#### 3.3.1 Event Preparedness Activation Notification Procedure

**Criteria:** Event Preparedness Activation notification procedures are initiated as early as 60 hours in advance of a pending Event which threatens the corporate data center.

**Actor:** IT DR Project Manager

**Timing:** 60 Hours Prior to Event Impact

**Action:** **IT DR Project Manager issues Event Preparedness Notification:**

1. Via email, the IT DR Project Manager will notify 'All IT Managers' as identified in the Company active directory that an Event Preparedness Alert has been issued.
2. Via email, the IT DR Project Mgr. will notify identified IT DR Team members (refer to the appendix of this document for a current listing of IT Team Members).
3. Via Outlook Calendar, establish a once daily recurring Event Preparedness Alert update meeting. Use the below DR conference number for telephone attendees:

Toll Free Dial In Number: (877)402-9753  
Int'l Access/Caller Paid Dial In Number: (636)651-3141  
ACCESS CODE: 1008220 HOST PASSWORD: 4210

### 3.3.2 Recovery Media Emergency Shipment Procedure

**Criteria:** Backup media is shipped on an emergency basis once a Event Preparedness Notification has been issued. The IT DR Project Manager will coordinate the decision with IT leadership and act according to leadership direction.

**Actor:** IT Infrastructure (Tape Backup Engineer) / IT DR Project Manager

**Timing:** 60 hours prior to predicted impact.

**Action:** **Emergency Shipment of DR Backup Media:**

1. Notify Tape Archive Vendor to initiate emergency shipment of backup media identified in section 3.2.3 of this document. Request expedited shipment via UPS and/or FedEx.
  - a. Archive Corporation Phone #: (813) 874-1577  
Archive Corporation Address: 6914 Asphalt Rd, Tampa FL 33614
  - b. SunGard Tape Receiving Address:  
SunGard Address: 777 Central Boulevard, Carlstadt, NJ 07072  
SunGard Contact: Orlando Rodriguez  
SunGard Phone #: 201-729-2389
2. Ship Critical Recovery media from corporate facility
  - a. Box on-site tapes
  - b. Weigh on-site tapes
  - c. Inventory on-site tapes
  - d. Request Shipping label from WellCare corporate shipping department. Ship via UPS or FedEx expedited delivery.
  - e. Address the shipment to:  
SunGard Address: 777 Central Boulevard, Carlstadt, NJ 07072  
SunGard Contact: Orlando Rodriguez  
SunGard Phone #: 201-729-2389
3. Notify SunGard of pending arrival of emergency media shipment
  - a. Email SunGard: Orlando.rodriquez@sungard.com
  - b. Call SunGard: Orlando Rodriguez @ 201-729-2389
4. SunGard inventories tapes at point of arrival and sends receipt inventory list to WellCare DR Project Manager to verify all shipped tapes are accounted for.
5. SunGard secures tape media in an area which restricts access to identified SunGard and/or WellCare associates.

### 3.3.3 I.T. DR Away Team Emergency Travel Procedure

**Criteria:** The I.T. DR Away Team travels under the direction and authorization of the CIO and EPC.

**Actor:** IT Away Team / IT DR Project Manager

**Timing:** 60 hours prior to predicted impact.

**Action:** **Designated I.T. Away Team Emergency Travel to Remote Recovery Location:**

1. Minimum Away Team Requirements
  - (1) Backup Engineer
  - (1) Server Engineer
2. I.T. Away Team travels per arrangements made in section 3.2.4 of this document.
3. I.T. Away Team is accountable for maintaining expenses per standard WellCare corporate travel policy.

### 3.4 Event Watch Milestone Procedures

Event Watch procedures are activated approximately 48 hours prior to event impact.

The following procedures are initiated per the authority of the Corporate Emergency Preparedness Committee and the Information Technology Chief Information Officer (CIO) or delegate(s).

#### 3.4.1 Event Watch Notification Procedure

**Criteria:** Event Watch notification procedures are initiated when a pending event continues to threaten the corporate data center.

**Actor:** IT DR Project Manager

**Timing:** 48 Hours Prior to Event Impact

**Action:** **IT DR Project Manager issues Event Watch Notification:**

1. Via email, the IT DR Project Manager will notify 'All IT Managers' as identified in the Company active directory that an Event Watch has been issued.
2. Via email, the IT DR Project Mgr. will notify identified IT DR Away Team members (refer to the appendix of this document for a current listing of IT Away Team Members).
3. Via Outlook Calendar, establish a twice daily recurring Event Watch update meeting. Use the below DR conference number for telephone attendees:

Toll Free Dial In Number: (877)402-9753

Int'l Access/Caller Paid Dial In Number: (636)651-3141

ACCESS CODE: 1008220 HOST PASSWORD: 4210

### 3.4.2 Establish IT DR Situation Room Procedure

The DR Project Manager will seek permission from the CIO to commandeer conference room 155 to serve as the IT DR Situation Room. All previously scheduled meetings in room 155 will be postponed, rescheduled to an alternate room, or cancelled. The DR Situation Room will be activated until the disaster scenario has ended or alternate facilities are identified.

**Criteria:** WellCare is preparing to or has issued a disaster declaration w/ the remote recovery vendor.

**Actor:** IT DR Project Manager

**Timing:** 48 hours prior to event.

**Action:** **Establish DR Situation Room:**

1. IT DR Project Manager contacts CIO Executive Administrator (refer to Appendix 5.3) to seek permission to commandeer either Ren 1 conference room 150 or room 155.
2. IT DR Project Manager, via email, notifies all I.T. DR team members of situation room activation.
3. IT DR Project Manager issues a 4 hour recurring meeting invite to all IT DR Response Team members.

### 3.4.3 Disaster Recovery Declaration Decision Procedure

**Criteria:** WellCare will issue a Disaster Recovery Declaration with the remote recovery vendor 48 hours prior to the event, or 24 hours in advance of mandatory / voluntary evacuation orders as directed by the local area Emergency Operating Center (EOC).

**Actor:** IT Away Team / IT DR Project Manager

**Timing:** 24 hours in advance of mandatory or voluntary local evacuation orders, or approximately 48 hours prior to event.

**Action:** **Disaster Declaration Decision:**

1. IT DR Project Manager to convene meeting w/ following IT Leaders:
  - CIO
  - VP Infrastructure
  - VP Process / Controls
  - VP Health and Channel Services
  - VP Data Mgmt
  - VP Core Processing
  - Director of Infrastructure
  - Director of Telecommunications / Network

The purpose of the meeting is to decide whether to issue an IT disaster declaration with the current remote recovery vendor.

2. The I.T. leaders in cooperation with the WellCare Emergency Preparedness Committee will decide to issue a disaster declaration with

the remote recovery vendor or to wait based on improving Event projections.

#### 3.4.4 Disaster Recovery Declaration w/ Remote Recovery Vendor Procedure

- Criteria:** The disaster recovery declaration with the remote recovery vendor is executed per the direction of the EPC and IT CIO.
- Actor:** IT DR Project Manager / IT Leadership
- Timing:** 24 hours in advance of mandatory or voluntary local evacuation orders (approximately 48 hours in advance of event).
- Action:** **Disaster Declaration w/ Remote Recovery Vendor:**
1. Refer to the Appendix 5.1 for a listing of current I.T. leaders who are authorized to declare a disaster with the remote recovery vendor (currently SunGard).
  2. One of the identified leaders must call and declare a disaster with the remote recovery vendor:
    - Call SunGard @ 1-866-722-1313
    - Whomever calls, must identify themselves as an Authorized Disaster Declaration Authority
    - Instruct the SunGard representative that the WellCare IT DR Project Manager is authorized to coordinate the remaining recovery activities. The current I.T. DR Project Manager is: W. Greg Brooks @ 1-813-810-4569 / [gbrooks@WellCare.com](mailto:gbrooks@WellCare.com)

#### 3.4.5 Remote DR Network Initiation

- Criteria:** A disaster declaration has been made with the remote recovery vendor and the IT DR Away team has arrived on-site at the remote recovery center.
- Dependencies:** Remote Vendor Cross-connection established
- Actor:** IT DR Network Engineer
- Timing:** 48 – 40 hours prior to impact
- Action:** **Initiate DR Network:**
1. Per the decision of the I.T. Incident Management Team (refer to Appendix 5.2), the DR Network Engineer will remotely connect to the DR Recovery network and configure the firewall to isolate the remote center hosts from the corporate data center. Refer to the detailed DR Network Recovery Procedure.
  2. Once the DR Network is configured, representatives from each DR infrastructure discipline will verify the DR network and the corporate I.T. resources to verify expected operation.
  3. DR Project Manager communicates to IT DR Recovery Team that the DR Network has been initialized.

#### 3.4.6 Execute Remote Data Center Recovery Procedure

Refer to section 4, Remote Data Center Recovery Procedures.

**Criteria:** WellCare will execute the remote data center recovery procedures immediately following the disaster declaration with the remote recovery vendor.

**NOTE:** If the IT DR Away Team has not previously traveled to the remote recovery site, refer to sections 3.2.4 and 3.3.3 of this document.

**Actor:** IT DR Team

**Timing:** 48 hours prior to event

**Action:** **IT DR Team Establish Remote DR Data Center:**

Refer to Section 4 of this document for the Remote Data Center Recovery Procedure(s).

### 3.4.7 Recovery Point Objective (RPO) Synchronization Procedure

There are multiple, critical databases that are recovered in support of the remote data center recovery. It is necessary to synchronize the recovery data 'point-in-time' to provide referential integrity between the various WellCare critical ERP databases. Point-in-time synchronization of critical data is accomplished via transmitting the database archive logs via the DR OC3 connection to the DR hosted environment. The database logs are applied to the respective databases to establish a common recovery point-in-time.

**Criteria:** A disaster declaration has been made with the remote recovery vendor and the IT DR Away team has arrived on-site at the remote recovery center.

**Dependencies:** 1.) Remote Vendor Cross-connection made  
2.) SAN storage allocated for DB archival logs

**Actor:** IT DR Team / IT DR Project Manager

**Timing:** 48 – 40 hours prior to event

**Action:** **Transmit Critical DB Archive Logs to Remote Recovery Facility:**

1. IT DR Project Manager convenes meeting w/ appropriate Incident Team members (refer to Appendix 5.2).
2. Based on the recovery prioritization matrices in Section 4.2 of this document, the above identified managers will identify the required actions necessary to provide minimal loss of production data.
3. DR Project Manager documents and communicates the decision notes and actual strategy to all DR Response Team members and Incident Management leaders.

## 3.5 Event Warning Milestone Procedures

Event Warning procedures are activated 24 hours in advance of Event impact.

The following procedures are initiated per the authority of the Corporate Emergency Preparedness Committee and the Information Technology Chief Information Officer (CIO) or delegate(s).

### 3.5.1 Event Warning Notification Procedure

**Criteria:** An Event Warning Notification is executed 24 hours in advance of event.

**Actor:** IT DR Project Manager

**Timing:** 24 hours prior to event

**Action: Issue Event Warning Notification:**

1. Via email, the IT DR Project Manager will notify 'All IT Managers' as identified in the Company active directory that a Event Warning has been issued.
2. Via email, the IT DR Project Mgr. will notify identified IT DR Team members (refer to the appendix of this document for a current listing of IT DR Team Members).
3. Via Outlook Calendar, establish a four times daily recurring Event Warning update meeting. Use the below DR conference number for telephone attendees:

Toll Free Dial In Number: (877) 402-9753

Int'l Access/Caller Paid Dial In Number: (636)651-3141

ACCESS CODE: 1008220 HOST PASSWORD: 4210

## 4 I.T. DISASTER RECOVERY PROCEDURES

The recovery procedures for Event scenarios are the same.

### 4.1 Post-Disaster Corporate Damage Assessment Procedure

Post-disaster damage assessment is initiated as soon as safely possible after the disaster impact.

**Criteria:** Corporate campus is directly or in-directly impacted by a disaster which renders the corporate data center non-functional.

**Actor:** EPC / IT Leadership / IT DR Project Manager / IT Incident Management Team

**Timing:** As soon as safely possible 8 – 12 hours after event impact

**Action:** **Inspect Corporate I.T. Assets post-disaster:**

1. IT DR Project Manager contacts IT Disaster Incident Management Team via call-out and email, and establishes a teleconference using the below bridge:

Toll Free Dial In Number: (877) 402-9753  
 Int'l Access/Caller Paid Dial In Number: (636)651-3141  
 ACCESS CODE: 1008220 HOST PASSWORD: 4210

2. IT DR Project Manager Coordinates the corporate campus I.T. Disaster Damage Assessment w/ facilities. Refer to the table below:

Name	Contact Information
Ken Van Stedum	<a href="mailto:Ken.VanStedum@WellCare.com">Ken.VanStedum@WellCare.com</a> BB: 813-317-0053
Frank Garced	<a href="mailto:fgarced@WellCare.com">fgarced@WellCare.com</a> BB: 813-454-9197
Alex Valdes	<a href="mailto:Alex.valdes@WellCare.com">Alex.valdes@WellCare.com</a> 813 290 6200 x1033

**Table 2: Facilities Contacts**

3. Refer to Appendix 5.2 for a listing of IT Disaster Incident Management Team members.
4. The IT DR Incident Management team identifies a safe meeting spot and agrees on a specified time to meet.
5. The IT DR Incident Management Team inspects the corporate data center facilities to determine extent of damage and projected recovery time.
6. Via email and/or call-out, the IT DR Project Manager will notify 'All IT Managers' as to the results of the IT Damage Assessment

7. Based on the IT DR Damage Assessment, either begin the recovery of the corporate data center, or initiate the remote recovery procedures as identified in this document.
8. Via email, the IT DR Project Mgr. will notify identified IT DR Team members (refer to the appendix of this document for a current listing of IT DR Team Members).
9. The IT DR Incident Managers will issue a report to the IT Executive Leaders, as well as to the Corporate Emergency Preparedness committee.

#### 4.2 Critical Applications Recovery Sequence

WellCare systems are recovered in the following phases:

- DR Phase I
  - DR network; i.e., in-bound and out-bound managed internet services, global DR WAN, DR LAN, etc.
  - DR Infrastructure; i.e., storage, active directory, citrix, email, etc.
  - Customer facing applications; i.e., corporate web-site, etc.
  - Critical ERP systems; i.e, Peradigm, Oracle Financials, etc.
  - Vendor facing applications; i.e., Softheon, E2FUI, EMMA, DER, In-bound / out-bound faxing, etc.
- DR Phase II
  - Channel Communications; i.e., EDI, Secure FTP, BizTalk, etc.
  - Integration Services; i.e., Enterprise Service Bus, .Net Services, etc.
  - Batch Services: i.e., Enterprise Scheduler (AutoSys), Batch Jobs, etc.
- DR Phase III
  - Surround Applications; i.e., Field Magic, CPR, etc.
  - Legacy email (phased, prioritized recovery)
  - Reporting environments

##### 4.2.1 DR Phase I Recovery Priority Matrix

The DR Phase I recovery efforts focus on establishing the technology infrastructure and framework from a network, server and storage perspective, and integration services (ESB), as well as recovering critical customer facing, vendor facing and corporate ERP systems.

Refer to the DR Phase I Data Center Recovery matrix below for the recovery priority and sequence for the DR Phase I recovery efforts:

DR Critical System	Recovery Sequence	Pro-active Response (RTO)*	Re-active Response (RTO)**	Recovery Point Objective (RPO)
DR Network	1.0	4 – 5days	6-7days	N/A
DR Infrastructure	2.0	4 – 5days	6-7days	N/A

DR Critical System	Recovery Sequence	Pro-active Response (RTO)*	Re-active Response (RTO)**	Recovery Point Objective (RPO)
DR Backup / Restore Environment	2.1	4 – 5days	6-7days	24hrs
Active Directory	2.2	4 – 5days	6-7days	24hrs
Citrix	2.3	4 – 5days	6-7days	N/A
MS Exchange (email)	2.4	4 – 5days	6-7days	No Legacy Email
Peradigm	3.0	4 – 5days	6-7days	24hrs
Oracle Financials	4.0	4 – 5days	6-8days	24hrs
Corporate Web	5.0	4 – 5days	6-8days	24hrs
SharePoint	6.0	4 – 5days	6-8days	24hrs
SideWinder	7.0	4 – 5days	6-8days	24 hrs
DER	8.0	4 – 5days	6-8days	24hrs
EMMA	9.0	4 – 5days	6-8days	24hrs
Softheon	10.0	4 – 5days	6-8days	24hrs
RightFax	11.0	4 – 5days	6-8days	N/A
OmniFlow	12.0	4 – 5days	6-8days	24hrs
Enterprise Service Bus	14	4 – 5days	6-8days	N/A
.NET Web Services	15	4 – 5days	6-8days	N/A
E2FUI	13.0	4 – 5days	6-8days	24hrs

**Table 3: Phase I System Recovery Sequence**

#### 4.2.2 DR Phase II Recovery Priority Matrix

The DR Phase II recovery efforts focus on establishing the channel services (EDI), batch processing services (AutoSys). Additional operational support systems are also recovered during the Phase II Remote Data Center Recovery Process.

Refer to the DR Phase II Data Center Recovery matrix below for the recovery priority and sequence for the DR Phase II recovery efforts:

DR Critical System	Recovery Sequence	Pro-active Response (RTO)*	Re-active Response (RTO)**	Recovery Point Objective (RPO)
EDI GateWay	16	6-8days	8-10days	N/A

**NOTICE**

DR Critical System	Recovery Sequence	Pro-active Response (RTO)*	Re-active Response (RTO)**	Recovery Point Objective (RPO)
Biz-Talk	17	6-8days	8-10days	N/A
X-Engine	18	6-8days	8-10days	N/A
Secure FTP	19	6-8days	8-10days	N/A
AutoSys (Enterprise Scheduler)	20	6-8days	8-10days	N/A
Robo-cops	21	6-8days	8-10days	N/A
Check-run	22	6-8days	8-10days	N/A

**Table 4: Phase II System Recovery Sequence**

#### 4.2.3 DR Phase III Recovery Priority Matrix

The DR Phase III recovery efforts focus on recovering additional operational support systems, restoring legacy email, and scaling the environment for performance.

Refer to the DR Phase III Data Center Recovery matrix below for the recovery priority and sequence for the DR Phase III recovery efforts:

DR Critical System	Recovery Sequence	Pro-active Response (RTO)*	Re-active Response (RTO)**	Recovery Point Objective (RPO)
AutoLetters	23	13-15days	15- 17days	N/A
WinStrat	24	13-15days	15- 17days	N/A
Field Magic	25	13-15days	15- 17days	24hrs
Cactus	26	13-15days	15- 17days	24hrs
CERET	27	13-15days	15- 17days	N/A
WFCE	28	13-15days	15- 17days	N/A
CPR	29	13-15days	15- 17days	24hrs
Legacy Email	30	13-15days	15- 17days	N/A

**Table 5: Phase III System Recovery Sequence**

**NOTICE**

### 4.3 Remote Data Center Recovery Procedures

The procedures prescribed below are expected to be performed by qualified, corporate IT engineers who are versed in the DR Remote Center recovery design and execution.

This document is supplemented by specific recovery procedures for each identified critical system. Accordingly, where applicable, procedures within this document will reference the detailed critical system recovery procedure. All detailed recovery procedures are stored electronically on the SunGard Recovery Portal at [www.mysungard.com](http://www.mysungard.com).

Identified critical applications are recovered in accordance to the sequence dictated in Section 4.2 Critical Applications Recovery Sequence.

#### 4.3.1 Execute DR Network Recovery Procedures

**Criteria:** 1.) WellCare has issued a disaster declaration with the current remote recovery vendor.  
2.) The SunGard network cross connect has been established.

**Actor:** DR Network Engineer / IT DR Project Manager

**Timing:** 48 hours prior to impact / As soon as possible post-disaster

**Action:** **Remote DR Network Recovery:**

1. Pre-disaster – 48 hours prior to impact, perform the remote DR network initiation per Section 3.4.5 of this document.
2. Post-disaster – as soon as safely possible, perform the remote DR network initiation per Section 3.4.5 of this document.

#### 4.3.2 Configure DR Host Servers

**Criteria:** 1.) Remote DR network has been initiated.  
2.) The SunGard network cross connect has been established.  
3.) Remote recovery vendor shared resources have been allocated.

**Actor:** DR Unix / Linux / Window Engineers

**Timing:** Immediately: once cross-connect is made; remote DR network has been initialized; and shared resources have been allocated.

**Action:** **Configure DR Host Servers:**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal, configure host servers; i.e., host name, IP address, patch levels, ancillary software, etc.
2. DR Infrastructure Engineers verify host server configuration.

#### 4.3.3 Configure / Allocate Storage

**Criteria:** 1.) Remote DR network has been initiated.  
2.) The SunGard network cross connect has been established.  
3.) Remote recovery vendor shared resources have been allocated.

**Actor:** DR Storage Engineers

**Timing:** Immediately, once cross-connect is made; remote DR network has been initialized; and shared resources have been allocated.

**Action: Configure / Allocate DR Storage (SAN)**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal, configure and allocate SAN storage to the appropriate hosts.
2. DR Infrastructure Engineers verify storage allocation and functionality.

**4.3.4 Execute Citrix Recovery Procedures**

The virtual Citrix image is pre-staged in the recovery site managed services rack. Once the DR Infrastructure is allocated and configured, the Citrix engineer will replicate the Citrix virtual image to accommodate 3000 remote users.

- Criteria:**
- 1.) Remote DR network has been initiated.
  - 2.) The SunGard network cross connect has been established.
  - 3.) Remote recovery vendor shared resources have been allocated.

**Actor:** DR Citrix Engineers

**Timing:** Immediately, once cross-connect is made; remote DR network has been initialized; shared resources have been allocated, and servers configured.

**Action: Establish Remote DR Citrix Farm**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal, restore initial Citrix image.
2. Continue scaling Citrix to accommodate 3000 remote connections.
3. Citrix engineers verify successful recovery.

**4.3.5 Execute Exchange Recovery Procedures**

Exchange ( MS Outlook ) is built new at the time of declaration once the infrastructure has been configured. The new build will include all MS Active Directory accounts and a script will be run to recover all public folders. The initial recovery of MS Exchange will not include legacy email. Legacy email, as required, will be restored in Phase III of the remote facility recovery.

- Criteria:**
- 1.) Remote DR network has been initiated.
  - 2.) The SunGard network cross connect has been established.
  - 3.) Remote recovery vendor shared resources have been allocated.

**Actor:** DR Exchange Engineer

**Timing:** Immediately, once cross-connect is made; remote DR network has been initialized; and shared resources have been allocated.

**Action: Build DR Exchange Server**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal, install and configure MS Exchange.
2. Record start and end times.
3. Run scripts to re-build all existing Active Directory accounts and public folders.
4. DR Exchange Engineer verifies storage allocation and functionality.

#### 4.3.6 Execute Veritas Recovery Procedures

Veritas Netback-up is pre-installed and configured in the recovery site managed services rack. The remote facility houses the DR\_CritBack server domain. The critical catalog is replicated to the DR CritBack domain each time the catalog is backed-up to tape.

**Criteria:** 1.) Remote DR network has been initiated.  
2.) The SunGard network cross connect has been established.  
3.) Remote recovery vendor shared resources have been allocated.

**Actor:** DR Back-up Engineer

**Timing:** Immediately: once cross-connect is made; remote DR network has been initialized; and shared resources have been allocated and configured.

**Action: Verify DR Backup Domain**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal, verify functionality of DR\_CritBack domain.
2. Record start and stop times.
3. If necessary, import the most current critical backup catalog.
4. DR Backup Engineer verifies successful restore of critical catalog.

#### 4.3.7 Restore Critical System Back-up Images

**NOTE:** Use care in the handling of the magnetic tape media during all phases of shipment and recovery activity. Mishandling the magnetic tapes may result in read errors and catastrophic failures.

**Criteria:** 1.) Remote DR network has been initiated.  
2.) The SunGard network cross connect has been established.  
3.) Remote recovery vendor shared resources have been allocated.  
4.) CritBack Domain is up and critical catalog is recovered.

**Actor:** DR Back-up Engineer

**Timing:** Immediately after the DR Critical Catalog is imported.

**Action: Restore Critical System Back-up Images**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal and the recovery sequence identified in Section 4.2 of this document, restore the critical systems to the identified host.
2. Record 'all' start and end times.
3. Monitor tape restore for tape read errors. If tape read errors occur, immediately escalate to the SunGard recovery coordinator and determine corrective action.
4. Verify critical restores.

#### 4.3.8 Recover Critical Applications

Once the back-up image is restored, the application(s) are recovered. Critical application recovery includes 'standing' up the application servers, to include middleware and network connectivity.

- Criteria:**
- 1.) Remote DR network has been initiated.
  - 2.) The SunGard network cross connect has been established.
  - 3.) Remote recovery vendor shared resources have been allocated.
  - 4.) CritBack Domain is up and critical catalog is recovered.
  - 5.) Critical Back-up for respective system is fully restored from tape.

**Actor:** DR Application Engineer / DBA / DR Infrastructure Engineer

**Timing:** Immediately after the DR Critical System Back-up is recovered.

**Action: Recover and Verify Critical Applications**

1. Per the detailed recovery procedures stored on the SunGard Recovery Portal and the recovery sequence identified in Section 4.2 of this document, recover the critical systems immediately once the back-up image has been restored.
2. Record 'all' start and end times.
3. Verify critical application is functional.

## 5 APPENDIX

### 5.1 SunGard Disaster Declaration Authority List

Refer to the list below for the WellCare IT leaders who are authorized to declare a disaster w/ SunGard.

Name	Title / Contact
Mark Lantzy	CIO mlantzy@wellcare.com
Paul Kohler	VP, IT Infrastructure pkohler@wellcare.com
Tim Craig	Dir., IT Telco / Network <a href="mailto:tcraig@WellCare.com">tcraig@WellCare.com</a>
Bob Klopotek	VP, Systems Delivery Bob.klopotek@wellcare.com

Exhibit 1: SunGard Disaster Declaration List

### 5.2 IT DR Incident Management Team List

Refer to the table below for the IT DR Incident Management List:

Disaster Recovery Role	Name / Title / Contact
IT DR Incident Manager	Tom Potts / Mgr. IT Unix / Linux / Storage <a href="mailto:tpotts@WellCare.com">tpotts@WellCare.com</a> CP: 813-206-3593
IT DR Incident Manager	Tim Craig / Dir., IT Telco / Network <a href="mailto:tcraig@WellCare.com">tcraig@WellCare.com</a> CP: 727-421-7108
IT DR Situation Manager	W. Greg Brooks / IT DR Project Mgr <a href="mailto:gbrooks@WellCare.com">gbrooks@WellCare.com</a> / CP: 813 810 4569
IT DR Incident Mgt Team	Randy Dougherty / IT Network Mgr <a href="mailto:rdougherty@WellCare.com">rdougherty@WellCare.com</a> CP: 813 810 4738
IT DR Incident Mgt Team	Todd Lightbody / Mgr. DBA <a href="mailto:tlightbody@WellCare.com">tlightbody@WellCare.com</a> CP: 813 326 5376
IT DR Incident Mgt Team	Deby McCourt / Mgr. IT Help Desk <a href="mailto:dmccourt@WellCare.com">dmccourt@WellCare.com</a> CP: 813 598 6248
IT DR Incident Mgt Team	Mori Chipi / Mgr. IT Operations <a href="mailto:mchipi@WellCare.com">mchipi@WellCare.com</a> CP:

**NOTICE**

IT DR Incident Mgt Team	Michael Longo / Mgr. IT Telco <a href="mailto:mlongo@WellCare.com">mlongo@WellCare.com</a>
-------------------------	---

Table A1: I.T. Incident Management Team

### 5.3 IT DR Team List

Refer to the table below for a listing of IT DR Team Members:

Name / Title / Contact	Responsibilities
Glenda Harmeling / DR Exec Administrator <a href="mailto:gharmeli@wellcare.com">gharmeli@wellcare.com</a> 813-206-3896	<ol style="list-style-type: none"> <li>1. I.T. Organizational Chart</li> <li>2. Emergency CIO contact</li> </ol>
Oscar Galdona / Network Engineer <a href="mailto:ogaldona@WellCare.com">ogaldona@WellCare.com</a> cp: 813-464-0723	<ol style="list-style-type: none"> <li>1. Manage DR Network</li> <li>2. Establish DR VPN Profiles for DR Team</li> <li>3. Execute DR Network Initiation Procedures</li> </ol>
Larry Church / Unix Engineer <a href="mailto:lchurch@WellCare.com">lchurch@WellCare.com</a> cp: 813-843-5865	<ol style="list-style-type: none"> <li>1. Unix Critical System Recovery</li> <li>2. Back-up Environment Recovery</li> <li>3. Back-up Restores</li> </ol>
Joe Cipolla / Linux Engineer <a href="mailto:jcipolla@WellCare.com">jcupolla@WellCare.com</a> cp: 813-206-1775	<ol style="list-style-type: none"> <li>1. Linux Critical System Recovery</li> </ol>
Greg Hatch / Windows Engineer <a href="mailto:ghatch@WellCare.com">ghatch@WellCare.com</a> cp: 813-421-4734	<ol style="list-style-type: none"> <li>1. Restore MS Exchange</li> <li>2. DNS Updates</li> <li>3. DR Infrastructure Configuration</li> </ol>
Kevin Young / Windows Engineer <a href="mailto:kyoung@WellCare.com">kyoung@WellCare.com</a> cp: 813-362-7647	<ol style="list-style-type: none"> <li>1. DR Emergency Media Shipment / Return</li> <li>2. Back-up Environment Recovery</li> <li>3. DR Infrastructure Configuration</li> </ol>
Naresh Viradiya / DBA <a href="mailto:nviradiya@WellCare.com">nviradiya@WellCare.com</a> cp: 813-810-6512	<ol style="list-style-type: none"> <li>1. DR Database Management</li> <li>2. Peradigm Database Restore</li> <li>3. Replication Services</li> </ol>
Ravi Ainpudi / DBA <a href="mailto:rainpudi@WellCare.com">rainpudi@WellCare.com</a> cp: 813-390-9929	<ol style="list-style-type: none"> <li>1. DR Database Management</li> <li>2. Replication Services</li> </ol>
Louis Kapp / DBA <a href="mailto:lkapp@WellCare.com">lkapp@WellCare.com</a> cp: 813 767-3069	<ol style="list-style-type: none"> <li>1. SharePoint Database Recovery</li> </ol>
Prasad Kodali / DBA <a href="mailto:pkodali@WellCare.com">pkodali@WellCare.com</a> cp: 813-382-3222	<ol style="list-style-type: none"> <li>1. Oracle Financials Database Restore</li> </ol>
Stephen Korda / Enterprise Storage <a href="mailto:skorda@WellCare.com">skorda@WellCare.com</a> cp: 813-841-1168	<ol style="list-style-type: none"> <li>1. Configure / Allocate DR Storage</li> </ol>

Table A2: I.T. Disaster Recovery Team

**NOTICE**