Program Memorandum Intermediaries/Carriers

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal AB-01-171 **Date: NOVEMBER 29, 2001**

CHANGE REQUEST 1929

SUBJECT: Request for Contractor's Business Contingency Plan (BCP)-January 15,2002

Applicability
This Program Memorandum (PM) applies to all carriers, intermediaries, their data centers, DMERCs and standard systems maintainers.

Background
In the spring of 1998, the President issued a directive to collect data on the Federal government's critical infrastructure. The directive is called the Presidential Decision Directive 63 (PDD63). PDD63 was issued to initiate all the measures necessary to quickly eliminate any significant vulnerability to the nation's critical infrastructures. PDD63 requires assessments to be performed of the services rendered by external business partners of federal agencies. The assessments will be used to determine if Medicare assets are being safeguarded from threats and vulnerabilities.

The PDD63 requirements were later incorporated into the Medicare core security requirements. Specifically, the CMS/Business Partner Systems Security Manual (www.hcfa.gov/extpart) directed the preparation of BCP, but did not require that the plan be submitted to CMS.

The CMS Business Partner Systems Security Manual essentially affirms our prior (now obsolete) guidance in the Medicare Intermediary Manual and Medicare Carrier Manual that requires preparation of a BCP, i.e, the requirement in the Business Partners Systems Security manual for a BCP is not a new requirement. Given recent events we have determined that a copy of this documentation needs to be on file at CMS. Accordingly, we are asking you to submit your Medicare BCP to CMS by January 15, 2002.

Submission Format:
Ideally, your BCP already follows the outline listed in Appendix C of the HCFA/Business Partner Systems Security Manual. If not in this format, you should not revise or change the contingency plan. However, at a minimum, your contingency plan should address the seven points listed on page 11 and 12 of Appendix "C", as summarized below. Definitions for the service components, operating components, and all components are listed in appendix C.

1. Management Summary and Recommendations: Also, address business continuity issues here. (Service components, operating components)

2. Phase One: Response-
   - List of names and numbers to phone in various contingencies. (Service components)
   - List of possible contingencies showing who to call for help and how employees should respond (Service components and outside sources such as police and fire departments):
     - Small fires that are local and easily contained;
     - Any fire in danger of spreading or producing noxious fumes;
     - Illness or injury;
     - Civil disorder, unruly demonstrations, vandalism, sabotage, strike, job action, etc.;
     - Bomb threat and search;
     - Storms posing imminent danger;
     - Earthquakes;
     - Explosions;
     - Power, heating, air-conditioning failures;
   - Coded actions indicating components' plans and involvement. (All components)
   - List of names and home addresses and phone numbers of each component's employees. (All components)
   - List of names of members of each component's emergency response team. (All components)

3. Phase Two: Backup-
   - Backup agreements showing what facilities are available under what conditions and for how long. (Service components)
   - Description of the facilities, equipment, and supplies needed for each component's vital operations. (All components)
   - Coded actions indicating each component's plans and involvement. (All components)
   - Lists of names of members of each component's backup team. (All components requiring backup operations)

4. Phase Three: Recovery-
   - A statement showing the general availability of suitable facilities in the area, plus names and numbers of realtors to contact. (Service components, outside sources)
   - A statement describing the processes used in securing new facilities, equipment and supplies, including names and numbers of those involved and the recovery function and responsibilities of each. (Service components)
   - Coded actions indicating each component's recovery plans and involvement. (All components)
   - List of names of members of each component's recovery team. (All components)

5. Record of Recommendations: Approval, denial, and implementation schedule.

6. Attachments: Complete equipment inventories, lists of computer software, systems and program documentation, prioritized computer schedules, list of all forms, list of all supplies, copy of current office directory, and lists of communications requirements, especially relating to computer networks. (Service components and operating components).

7. Record of Testing and Updating: (Service components and operating components).

If you have an existing Corporate BCP, which covers your Medicare line of business, you do not have to revise or change the Contingency Plan to accommodate the CMS format. You may, instead, prepare a comparative crosswalk table of your Corporate BCP format to the above format.

Submission Requirements
Submit your BCP as follows:

Document	**# of Copies**	**Format**
Signed Transmittal letter This letter must be signed and approved by the appropriate corporate officials.	2	Paper
Business Contingency Plan	2	CD-ROM (only), e-mail attachments will not be accepted.
Crosswalk Table (if required)	2	CD-ROM

One copy of the Transmittal letter and Business Contingency Plan should be sent by parcel delivery service to:

Centers of Medicare & Medicaid Services
Office of Information Services
Attention: Diane Keiser
Mail Stop: N2-14-17
7500 Security Boulevard
Baltimore, MD 21223

Send the second copy of the Transmittal letter and Business Contingency Plan by parcel delivery service to your respective Consortium Contractors Management Officer (CCMO). The addresses for the CCMOs are:

Pat Volk, Northeast
CCMO
Philadelphia Regional Office
Suite 216, The Public Ledger Building
150 South Independence Mall West
Philadelphia, PA 19106
E-Mail: PVolk@cms.hhs.gov

John Delaney, Southern
CCMO
Dallas Regional Office
1301 Young Street
Dallas, TX 75202
E-Mail: JDelaney@cms.hhs.gov

Daly Vargas, Midwest
CCMO
Chicago Regional Office
233 North Michigan Avenue, Suite 600
Chicago, IL 60601
E-Mail: DVargas@cms.hhs.gov

Alysson Blake, Western
CCMO
75 Hawthorne Street, 4th and 5th Floors
San Francisco, CA 94105-3901
E-Mail: ABlake@cms.hhs.gov

Send shipments by parcel delivery service.

CMS Security

CMS will observe strict procedures for safeguarding the Contractor's BCP information. Once CMS receives the Contractor's BCP, we will place the BCP into a controlled environment. CMS has defined procedures for the proper and secure receipt, control, handling, storage, and access for each of the contractor's submissions. These procedures include restricting access to only authorized CMS employees.

Disclosures under the Freedom of Information Act (FOIA)

Requests from members of the public for copies of contractor BCPs will be handled under FOIA (5 U.S.C. § 552) rules. Accordingly, under exemption 4 of FOIA (5 U.S.C. § 552 (b)(4)), CMS will protect any information within the BCP (or attachments thereto) that constitutes a trade secret or privileged or confidential commercial and financial information, as such terms are interpreted under the FOIA and applicable case law. Also, under exemption 6 of FOIA (5 U.S.C. § 552 (b)(6)), CMS will protect information that is of a highly sensitive personal nature if disclosure of such information would constitute a clearly unwarranted invasion of personal privacy of one or more persons.

The *effective date* for this Program Memorandum (PM) is November 29, 2001.

The *implementation date* for this PM is January 15, 2002.

These instructions should be implemented within your current operating budget.

This PM may be discarded after January 15, 2003.

If you have any questions, contact Rason Taru at (410) 786-3356.