exposure of computer equipment and thus achieve an optimum level of protection and security for the EDB system. For computerized records, safeguards have been established in accordance with the Department of Health and Human Services (HHS) standards and National Institute of Standards and Technology guidelines, e.g., security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management (IRM) Circular #10, Automated Information Systems Security Program; CMS Automated Information Systems (AIS) Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

RETENTION AND DISPOSAL:

Records are maintained for a period of 15 years.

SYSTEM MANAGERS AND ADDRESS:

Director, Health Plan Policy Group, Center for Beneficiary Choices, CMS, 7500 Security Boulevard, S1–05–06, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, health insurance claim number, address, date of birth, and sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES:

The subject individual should contact the systems manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with department regulation 45 CFR 5b.7).

RECORD SOURCE CATEGORIES:

The data contained in these records are furnished by the individual, or in the case of some MSP situations, through third party contacts. There are cases, however, in which the identifying information is provided to the physician by the individual; the physician then adds the medical information and submits the bill to the carrier for payment. Updating information is also obtained from the Railroad Retirement Board, and the Master Beneficiary Record maintained by the SSA.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–1526 Filed 1–22–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare and Medicaid Services

Privacy Act of 1974; Report of Modified or Altered System

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) (formerly the Health Care Financing Administration).

ACTION: Notice of modified or altered System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter a system of records, ''Common Working File (CWF),'' System No. 09–70–0526. We propose to delete published routine uses number 1 authorizing disclosure to claimants and their authorized representatives, number 3 authorizing disclosure to third party contacts to establish or verify information, number 4 authorizing disclosure to the Treasury Department for investigating alleged theft, number 5 authorizing disclosure to the United States Postal Service (USPS), number 6 authorizing disclosure to the Department of Justice (DOJ) to combat fraud and abuse, number 7 authorizing disclosure to the Railroad Retirement Board (RRB), number 9 authorizing disclosure to State Licensing Board for review of unethical practices, number 12 authorizing disclosure to state welfare departments, number 14 authorizing disclosure to state audit agencies, number 16 authorizing disclosure to peer review groups to assist with questions of medical necessity, number 17 authorizing disclosure to physicians and other supplier of services attempting to validate amounts of individual items, number 18 authorizing disclosure to senior citizen volunteers to assist beneficiaries, number 19 authorizing disclosure to a contractor to recover erroneous Medicare payments, number 20 authorizing disclosure to state and other governmental Workers' Compensation Agencies, number 23 authorizing disclosure to an agency of a state government or established by law, and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA).

Disclosures permitted under routine uses number 4, 5, 7, 9, 12, 14, 20, 23, and to the SSA will be made a part of proposed routine use number 2. Proposed routine use number 2 will allow for release of information to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' Disclosures permitted under published routine uses number 1, 2, 3, and 18 will now be covered by proposed routine use number 3, which will allow for release of information to ''third party contacts.'' Disclosure to ''other insurers and group health plans'' contained in published routine use 21 has been broaden to include similar groups with similar activities. This routine use will be renumbered as proposed routine use number 6. Disclosures permitted under routine use number 6 will be covered by proposed routine use number 11, which will permit the release of data to other Federal agencies for the purposes of combating fraud and abuse. Disclosures permitted under routine use number 10 will be made a part of proposed routine use number 4, which will permit the release of data to physicians and providers of services. Routine use number 16 is being deleted because the information listed in the routine use as being releasable ''at the request of the carrier to assist in the resolution of questions of medical necessity, utilization and overutilization,'' is no longer maintained in the CWF. Routine use number 17 is also being deleted because the activity listed in the routine use unnecessarily duplicates activities described in proposed routine use number 4. Disclosures permitted under routine use number 19 will now be covered by proposed routine use number 10, which will permit the release of data to a CMS contractor or grantee for the purposes of combating fraud and abuse. We propose to renumber published routine use number 22 as proposed routine use number 1 and modify the language to clarify the circumstances for disclosure to contractors and consultants. We will establish a new proposed routine use number 9 to allow disclosure to DOJ for the purpose of representing Agency employees involved in litigation.

The security classification previously reported as ''None'' will be modified to

reflect that the data in this system is considered to be ''Level Three Privacy Act Sensitive.'' We are modifying the language in the remaining routine uses to provide clarity to CMS's intention to disclose individual-specific information contained in this system. The routine uses will then be prioritized and reordered according to their usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization and to update language in the administrative sections to correspond with language used in other CMS systems of records.

The primary purpose of the system of records is to properly pay medical insurance benefits to or on behalf of entitled beneficiaries. Information in this system will also be released to: Support regulatory and policy functions performed within the Agency or by a contractor or consultant, another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent, third party contacts, providers and suppliers of services directly or through fiscal intermediaries or carriers, Peer Review Organizations (PRO) and Quality Review Organizations (QRO), insurance companies and other groups providing protection for their enrollees, or who are primary payers to Medicare in accordance with 42 U.S.C. 1395y (b), an individual or organization for research, evaluation, or epidemiological projects, support constituent requests made to a congressional representative, support litigation involving the Agency related to this system of records, and combat fraud and abuse in certain Federally funded health care programs. We have provided background information about the modified system in the ''Supplementary Information'' section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

EFFECTIVE DATES: CMS filed a modified or altered system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on January 15, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered system of records, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution, CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.–3 p.m., eastern time zone.

FOR FURTHER INFORMATION CONTACT: Richard Wolfsheimer, Health Insurance Specialist, Division of Fiscal Intermediary Systems and Common Working Files, Business Systems Operating Group, Office of Information Services, CMS, Room N2–09–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–6160.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System of Records

A. Statutory and Regulatory Basis For System of Records

In 1988, CMS modified an SOR under the authority of sections 1816, and 1874 of Title XVIII of the Act (the Act) (42 United States Code (U.S.C.) 1395h, and 1395kk). Notice of the modification to this system, ''Common Working Files, System No. 09–70–0526'' was published in the **Federal Register** (FR) at 53 FR 52806 (Dec. 29, 1988), an unnumbered routine use was added for the SSA at 61 FR 6645 (Feb. 21, 1996), three new fraud and abuse routine uses were added at 63 FR 38414 (July 16, 1998), and then at 65 FR 50552 (Aug. 18, 2000), two of the fraud and abuse routine uses were revised and a third deleted.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system contains information on Medicare beneficiaries, on whose behalf providers have submitted claims for reimbursement on a reasonable cost basis under Medicare Part A and B, or are eligible, and/or individuals whose enrollment in an employer group health benefits plan covers the beneficiary. Information contained in this system consist of billing for medical and other health care services, uniform bill for provider services or equivalent data in an electronic format, and MSP records containing other third party liability insurance information necessary for appropriate Medicare claims payment and other documents used to support payments to beneficiaries and providers of services. These forms contain the beneficiary's name, sex, health insurance claim number (HIC), address, date of birth, medical record number, prior stay information, provider name and address, physician's name, and/or identification number, warranty information when pacemakers are implanted or explanted, date of admission or discharge, other health insurance, diagnosis, surgical procedures, and a statement of services rendered for related charges and other data needed to substantiate claims.

B. Agency Policies, Procedures, and Restrictions on the Routine Use

The Privacy Act permits us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such disclosure of data is known as a ''routine use.'' The government will only release CWF information that can be associated with an individual as provided for under ''Section III. Proposed Routine Use Disclosure of Data in the System.'' Both identifiable and non-identifiable data may be disclosed under a routine use. We will only disclose the minimum personal data necessary to achieve the purpose of CWF. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. In general, disclosure of information from the system of records will be approved only for the minimum information necessary to accomplish the purpose of the disclosure only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, e.g., to properly pay medical insurance benefits to or on behalf of entitled beneficiaries.

2. Determines:

a. That the purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;

b. That the purpose for which the disclosure is to be made is of sufficient importance to warrant the effect and/or risk on the privacy of the individual that additional exposure of the record might bring; and

c. That there is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

3. Requires the information recipient to:

a. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

b. Remove or destroy at the earliest time all individually-identifiable information; and

c. Agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the CWF without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. We propose to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors or consultants who have been engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system of records and who need to have access to the records in order to assist CMS.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing a CMS function relating to purposes for this system of records.

CMS occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or consultant whatever information is necessary for the contractor or consultant to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or consultant from using or disclosing the information for any purpose other than that described in the contract and requires the contractor or consultant to return or destroy all information at the completion of the contract.

Carriers and intermediaries occasionally work with contractors to identify and recover erroneous Medicare payments for which workers' compensation programs are liable.

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent pursuant to agreements with CMS to:

a. Contribute to the accuracy of CMS's proper payment of Medicare benefits,

b. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds, and/or

c. Assist Federal/state Medicaid programs within the state.

Other Federal or state agencies in their administration of a Federal health program may require CWF information for the purposes of determining, evaluating, and/or assessing cost, effectiveness, and/or the quality of health care services provided in the state, to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided.

The Treasury Department may require CWF data for investigating alleged theft, forgery, or unlawful negotiation of Medicare reimbursement checks.

The USPS may require CWF data for investigating alleged forgery or theft of reimbursement checks.

The RRB requires CWF information to enable them to assist in the implementation and maintenance of the Medicare program.

SSA requires CWF data to enable them to assist in the implementation and maintenance of the Medicare program.

The Internal Revenue Service may require CWF data for the application of tax penalties against employers and employee organizations that contribute to Employer Group Health Plan or Large Group Health Plans that are not in compliance with 42 U.S.C. 1395y (b).

Disclosure under this routine use shall be used by state Medicaid agencies pursuant to agreements with HHS for administration of state supplementation payments for determinations of eligibility for Medicaid, for enrollment of welfare recipients for medical insurance under section 1843 of the Act, for quality control studies, for determining eligibility of recipients of assistance under Titles IV, and XIX of the Act, and for the complete administration of the Medicaid program. CWF data will be released to the state only on those individuals who are patients under the services of a Medicaid program within the state or who are residents of that state.

Occasionally state licensing boards require access to the CWF data for review of unethical practices or nonprofessional conduct.

We also contemplate disclosing information under this routine use in situations in which state auditing agencies require CWF information for auditing of Medicare eligibility considerations. Disclosure of physicians' customary charge data are made to state audit agencies in order to ascertain the corrections of Title XIX charges and payments. CMS may enter into an agreement with state auditing agencies to assist in accomplishing functions relating to purposes for this system of records.

State and other governmental workers' compensation agencies working with CMS to assure that workers' compensation payments are made where Medicare has erroneously paid and workers' compensation programs are liable.

3. To third party contacts (without the consent of the individuals to whom the information pertains) in situations where the party to be contacted has, or is expected to have information relating to the individual's capacity to manage his or her affairs or to his or her eligibility for, or an entitlement to, benefits under the Medicare program and,

a. The individual is unable to provide the information being sought (an individual is considered to be unable to provide certain types of information when any of the following conditions exists: the individual is confined to a mental institution, a court of competent jurisdiction has appointed a guardian to manage the affairs of that individual, a court of competent jurisdiction has declared the individual to be mentally incompetent, or the individual's attending physician has certified that the individual is not sufficiently mentally competent to manage his or her own affairs or to provide the information being sought, the individual cannot read or write, cannot afford the cost of obtaining the information, a language barrier exist, or the custodian of the information will not, as a matter of policy, provide it to the individual), or

b. The data are needed to establish the validity of evidence or to verify the accuracy of information presented by the individual, and it concerns one or more of the following: The individual's entitlement to benefits under the Medicare program; and the amount of reimbursement; any case in which the evidence is being reviewed as a result of suspected fraud and abuse, program integrity, quality appraisal, or evaluation and measurement of program activities.

Third parties contacts require CWF information in order to provide support for the individual's entitlement to benefits under the Medicare program; to establish the validity of evidence or to verify the accuracy of information presented by the individual or the representative of the applicant, and assist in the monitoring of Medicare claims information of beneficiaries, including proper reimbursement of services provided.

Senior citizen volunteers working in the carriers and intermediaries' offices to assist Medicare beneficiaries' request for assistance may require access to CWF information.

Occasionally fiscal intermediary/carrier banks, automated clearing houses, VANS, and provider banks, to the extent necessary transfer to providers electronic remittance advice of Medicare payments, and with respect to provider banks, to the extent necessary to provide account management services to providers using this information.

4. To providers and suppliers of services dealing through fiscal intermediaries or carriers for the administration of Title XVIII of the Act.

Providers and suppliers of services require CWF information in order to establish the validity of evidence, or to verify the accuracy of information presented by the individual as it concerns the individual's entitlement to benefits under the Medicare program, including proper reimbursement for services provided.

Providers and suppliers of services who are attempting to validate items on which the amounts included in the annual Physician/Supplier Payment List, or other similar publications are based.

5. To Peer Review Organizations (PRO) in connection with review of claims, or in connection with studies or other review activities, conducted pursuant to Part B of Title XI of the Act and in performing affirmative outreach activities to individuals for the purpose of establishing and maintaining their entitlement to Medicare benefits or health insurance plans.

PROs will work to implement quality improvement programs, provide consultation to CMS, its contractors, and to state agencies. PROs will assist the state agencies in related monitoring and enforcement efforts, assist CMS and intermediaries in program integrity assessment, and prepare summary information for release to CMS.

6. To insurance companies, underwriters, third party administrators (TPA), employers, self-insurers, group health plans, health maintenance organizations (HMO), health and welfare benefit funds, managed care organizations, other supplemental insurers, non-coordinating insurers, multiple employer trusts, liability insurers, no-fault medical automobile insurers, workers' compensation carriers or plans, other groups providing protection against medical expenses without the beneficiary's authorization, and any entity having knowledge of the occurrence of any event affecting (a) an individual's right to any such benefit or payment, or (b) the initial right to any such benefit or payment, for the purpose of coordination of benefits with the Medicare program and implementation of the MSP provision at 42 U.S.C. 1395y (b). Information to be disclosed shall be limited to Medicare utilization data necessary to perform that specific function. In order to receive the information, they must agree to:

a. Certify that the individual about whom the information is being provided is one of its insured or employees, or is insured and/or employed by another entity for whom they serve as a TPA;

b. Utilize the information solely for the purpose of processing the individual's insurance claims; and

c. Safeguard the confidentiality of the data and prevent unauthorized access.

Other insurers may require CWF information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided.

7. To an individual or organization for research, evaluation, or epidemiological projects related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.

The CWF data will provide for research, evaluations and epidemiological projects, a broader, longitudinal, national perspective of the status of Medicare beneficiaries. CMS anticipates that many researchers will have legitimate requests to use these data in projects that could ultimately improve the care provided to Medicare beneficiaries and the policy that governs the care.

8. To a Member of Congress or congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

Beneficiaries often request the help of a Member of Congress in resolving an issue relating to a matter before CMS. The Member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

9. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The Agency or any component thereof, or

b. Any employee of the Agency in his or her official capacity, or

c. Any employee of the Agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. The United States Government,

is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records is deemed by the Agency to be for a purpose that is compatible with the purposes for which the Agency collected the records.

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court or adjudicatory body involved.

10. To a CMS contractor (including, but not limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contract or grant with a third party to assist in accomplishing CMS functions relating to the purpose of combating fraud and abuse.

CMS occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or grantee whatever information is necessary for the contractor or grantee to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or grantee from using or disclosing the information for any purpose other than that described in the contract and requiring the contractor or grantee to return or destroy all information.

11. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to

investigate potential fraud or abuse in a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

Other agencies may require CWF information for the purpose of combating fraud and abuse in such Federally funded programs.

B. Additional Circumstances Affecting Routine Use Disclosures

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, published at 65 FR 82462 (12–28–00), as amended by 66 FR 12434 (2–26–01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.''

In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

IV. Safeguards

A. Administrative Safeguards

The CWF system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: The Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Office of Management and Budget (OMB) Circular A–130, Appendix III, ''Security of Federal Automated Information Resources.'' CMS has prepared a comprehensive system security plan as required by the OMB Circular A–130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems.'' Paragraphs A–C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

Authorized users: Personnel having access to the system have been trained in Privacy Act and systems security requirements. Employees and contractors who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. In addition, CMS is monitoring the authorized users to ensure against excessive or unauthorized use. Records are used in a designated work area or workstation and the system location is attended at all times during working hours.

To assure security of the data, the proper level of class user is assigned for each individual user as determined at the Agency level. This prevents unauthorized users from accessing and modifying critical data. The system database configuration includes five classes of database users:

- Database Administrator class owns the database objects; *e.g.,* tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- Quality Indicator Report Generator class has read-only access to all fields and tables;
- Policy Research class has query access to tables, but are not allowed to access confidential individual identification information; and
- Submitter class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards

All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the CWF system.

Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information System (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-on—Authentication is performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.
- Workstation Names—Workstation naming conventions may be defined and implemented at the Agency level.
- Hours of Operation—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the Agency level.
- Inactivity Log-out—Access to the NT workstation is automatically logged out after a specified period of inactivity.
- Warnings—Legal notices and security warnings display on all servers and workstations.
- Remote Access Services (RAS)—Windows NT RAS security handles resource access control. Access to NT resources is controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

C. Procedural Safeguards: All automated systems must comply with Federal laws, guidance, and policies for information systems security as stated previously in this section. Each automated information system should ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

V. Effect of the Modified System of Records on Individual Rights

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CMS will monitor the collection and reporting of CWF data. CWF information on individuals is completed

by contractor personnel and submitted to CMS through standard systems located at different locations. CMS will utilize a variety of onsite and offsite edits and audits to increase the accuracy of CWF data.

CMS will take precautionary measures (see item IV. above) to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure of identifiable data from the modified system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act.

CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of the disclosure of information relating to individuals.

Dated: January 14, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0525

SYSTEM NAME:

Common Working Files (CWF) System, HHS/CMS/OIS.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive.

SYSTEM LOCATION:

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850 and at CMS Regional Offices, CMS Intermediaries and Carriers, and at locations listed in Appendix A.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system contains information on Medicare beneficiaries, on whose behalf providers have submitted claims for reimbursement on a reasonable cost basis under Medicare Part A and B, or are eligible, and/or individuals whose enrollment in an employer group health benefits plan covers the beneficiary.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information contained in this system consist of billing for medical and other health care services, uniform bill for provider services or equivalent data in an electronic format, and Medicare Secondary Payer (MSP) records containing other third party liability insurance information necessary for appropriate Medicare claims payment and other documents used to support payments to beneficiaries and providers of services. These forms contain the beneficiary's name, sex, health insurance claim number (HIC), address, date of birth, medical record number, prior stay information, provider name and address, physician's name, and/or identification number, warranty information when pacemakers are implanted or explanted, date of admission or discharge, other health insurance, diagnosis, surgical procedures, and a statement of services rendered for related charges and other data needed to substantiate claims.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for the maintenance of this system of records is given under the authority of sections 1816, and 1874 of Title XVIII of the Social Security Act (42 United States Code (USC) 1395h, and 1395kk).

PURPOSE(S):

The primary purpose of the system of records is to properly pay medical insurance benefits to or on behalf of entitled beneficiaries. Information in this system will also be released to: support regulatory and policy functions performed within the Agency or by a contractor or consultant, another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent, third party contacts, providers and suppliers of services directly or through fiscal intermediaries or carriers, Peer Review Organizations (PRO), insurance companies and other groups providing protection for their enrollees, or who are primary payers to Medicare in accordance with 42 U.S.C. 1395y (b), an individual or organization for research, evaluation, or epidemiological projects, support constituent requests made to a congressional representative, support litigation involving the agency related to this system of records, and combat fraud and abuse in certain Federally funded health care programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OR USERS AND THE PURPOSES OF SUCH USES:

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the CWF without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary). This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, published at 65 FR 82462 (12–28–00), as amended by 66 FR 12434 (2–26–01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.'' We propose to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors or consultants who have been engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system of records and who need to have access to the records in order to assist CMS.

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent pursuant to agreements with CMS to:

a. Contribute to the accuracy of CMS's proper payment of Medicare benefits,

b. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds, and/or

c. Assist Federal/state Medicaid programs within the state.

3. To third party contacts (without the consent of the individuals to whom the information pertains) in situations where the party to be contacted has, or is expected to have information relating to the individual's capacity to manage his or her affairs or to his or her eligibility for, or an entitlement to, benefits under the Medicare program and,

a. The individual is unable to provide the information being sought (an individual is considered to be unable to provide certain types of information when any of the following conditions exists: the individual is confined to a mental institution, a court of competent jurisdiction has appointed a guardian to manage the affairs of that individual, a

court of competent jurisdiction has declared the individual to be mentally incompetent, or the individual's attending physician has certified that the individual is not sufficiently mentally competent to manage his or her own affairs or to provide the information being sought, the individual cannot read or write, cannot afford the cost of obtaining the information, a language barrier exists, or the custodian of the information will not, as a matter of policy, provide it to the individual), or

b. The data are needed to establish the validity of evidence or to verify the accuracy of information presented by the individual, and it concerns one or more of the following: the individual's entitlement to benefits under the Medicare program; and the amount of reimbursement; any case in which the evidence is being reviewed as a result of suspected fraud and abuse, program integrity, quality appraisal, or evaluation and measurement of program activities.

4. To providers and suppliers of services dealing through fiscal intermediaries or carriers for the administration of Title XVIII of the Act.

5. To Peer Review Organizations (PRO) in connection with review of claims, or in connection with studies or other review activities, conducted pursuant to Part B of Title XI of the Act and in performing affirmative outreach activities to individuals for the purpose of establishing and maintaining their entitlement to Medicare benefits or health insurance plans.

6. To insurance companies, underwriters, third party administrators (TPA), employers, self-insurers, group health plans, health maintenance organizations (HMO), health and welfare benefit funds, managed care organizations, other supplemental insurers, non-coordinating insurers, multiple employer trusts, liability insurers, no-fault medical automobile insurers, workers' compensation carriers or plans, other groups providing protection against medical expenses without the beneficiary's authorization, and any entity having knowledge of the occurrence of any event affecting (a) an individual's right to any such benefit or payment, or (b) the initial right to any such benefit or payment, for the purpose of coordination of benefits with the Medicare program and implementation of the MSP provision at 42 U.S.C. 1395y (b). Information to be disclosed shall be limited to Medicare utilization data necessary to perform that specific function. In order to receive the information, they must agree to:

a. Certify that the individual about whom the information is being provided is one of its insured or employees, or is insured and/or employed by another entity for whom they serve as TPA;

b. Utilize the information solely for the purpose of processing the individual's insurance claims; and

c. Safeguard the confidentiality of the data and prevent unauthorized access.

7. To an individual or organization for research, evaluation, or epidemiological projects related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.

8. To a Member of Congress or congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

9. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The Agency or any component thereof, or

b. Any employee of the Agency in his or her official capacity, or

c. Any employee of the Agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. The United States Government, is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records is deemed by the Agency to be for a purpose that is compatible with the purposes for which the Agency collected the records.

10. To a CMS contractor (including, but not limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

11. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained on paper, computer diskette and on magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by the beneficiary's name, HIC, and assigned unique physician identification number.

SAFEGUARDS:

CMS has safeguards for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data.

In addition, CMS has physical safeguards in place to reduce the exposure of computer equipment and thus achieve an optimum level of protection and security for the CWF system. For computerized records, safeguards have been established in accordance with the Department of Health and Human Services (HHS) standards and National Institute of Standards and Technology guidelines, e.g., security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management (IRM) Circular #10, Automated Information Systems Security Program; CMS Automated Information Systems (AIS) Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised) Appendix III.

RETENTION AND DISPOSAL:

Records are maintained in a secure storage area with identifiers. Records are closed at the end of the calendar year in which paid, held 2 additional years, transferred to Federal records center and destroyed after another 2 years.

SYSTEM MANAGERS AND ADDRESS:

Director, Division of Intermediary and Fiscal Systems, Business Systems Operations Group, Office of Information Services, CMS, 7500 Security Boulevard, Room N2–09–27, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, inquiries should addressed to the social security office nearest the requester's residence, the appropriate intermediary, the CMS regional office, or write to the system manager listed above. The entity contacted will require the system name, HIC, address, date of birth, and sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 Code of Federal Regulations (CFR) 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7).

RECORD SOURCE CATEGORIES:

Sources of information contained in this records system is furnished by the individual. In most cases, the identifying information is provided to the physician by the individual. Information is obtained from other CMS systems of records and data systems: Health Insurance Master Record, Intermediary Medicare Claims Records, Carrier Medicare Claims Records, MSP Record, Third Party Liability Record, Medicare Entitlement Record, Health Maintenance Organization Record, Hospice Record, and in the case of some MSP situations, through third party contacts. The medical information is provided by the providers of medical services.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

Appendix A. Health Insurance Claims

Medicare records are maintained at the HCFA Central Office (see section 1 below for the address). Health Insurance Records of the Medicare program can also be accessed through a representative of the HCFA Regional Office (see section 2 below for addresses). Medicare claims records are also maintained by private insurance organizations who share in administering provisions of the health insurance programs. These private insurance organizations, referred to as carriers and intermediaries, are under contract to the Health Care Financing Administration and the Social Security Administration to perform specific task in the Medicare program (see section three below for addresses for intermediaries, section four addresses the carriers, and section five addresses the Payment Safeguard Contractors.

1. Central Office Address

HCFA Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

2. HCFA Regional Offices

Boston Region—Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont. John F. Kennedy Federal Building, Room 1211, Boston, Massachusetts 02203. Office Hours: 8:30 a.m.–5 p.m.

New York Region—New Jersey, New York, Puerto Rico, Virgin Islands. 26 Federal Plaza, Room 715, New York, New York 10007, Office Hours: 8:30 a.m.–5 p.m.

Philadelphia Region—Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia. Post Office Box 8460, Philadelphia, Pennsylvania 19101. Office Hours:8:30 a.m.–5 p.m.

Atlanta Region—Alabama, North Carolina, South Carolina, Florida, Georgia, Kentucky, Mississippi, Tennessee. 101 Marietta Street, Suite 702, Atlanta, Georgia 30223, Office Hours: 8:30 a.m.–4:30 p.m.

Chicago Region—Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin. Suite A–824, Chicago, Illinois 60604. Office Hours: 8 a.m.–4:45 p.m.

Dallas Region—Arkansas, Louisiana, New Mexico, Oklahoma, Texas, 1200 Main Tower Building, Dallas, Texas. Office Hours: 8 a.m.–4:30 p.m.

Kansas City Region—Iowa, Kansas, Missouri, Nebraska. New Federal Office Building, 601 East 12th Street—Room 436, Kansas City, Missouri 64106. Office Hours: 8 a.m.–4:45 p.m.

Denver Region—Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming. Federal Office Building, 1961 Stout St—Room 1185, Denver, Colorado 80294. Office Hours: 8 a.m.–4:30 p.m.

San Francisco Region—American Samoa, Arizona, California, Guam, Hawaii, Nevada. Federal Office Building, 10 Van Ness Avenue, 20th Floor, San Francisco, California 94102. Office Hours: 8 a.m.–4:30 p.m.

Seattle Region—Alaska, Idaho, Oregon, Washington. 1321 Second Avenue, Room 615, Mail Stop 211, Seattle, Washington 98101. Office Hours 8 a.m.–4:30 p.m.

3. Intermediary Addresses (Hospital Insurance)

Medicare Coordinator, Assoc. Hospital Serv. Maine (ME BC), 2 Gannett Drive South, Portland, ME 04106–6911.

Medicare Coordinator, Anthem New Hampshire, 300 Goffs Falls Road, Manchester, NH 03111–0001.

Medicare Coordinator, BC/BS Rhode Island (RI BC), 444 Westminster Street, Providence, RI 02903–3279.

Medicare Coordinator, Empire Medicare Services, 400 S. Salina Street, Syracuse, NY 13202.

Medicare Coordinator, Cooperativa, P.O. Box 363428, San Juan, PR 00936–3428.

Medicare Coordinator, Maryland B/C, P.O. Box 4368, 1946 Greenspring Ave., Timonium, MD 21093.

Medicare Coordinator, Highmark, P5103, 120 Fifth Avenue Place, Pittsburgh, PA 15222–3099.

Medicare Coordinator, United Government Services, 1515 N. Rivercenter Dr., Milwaukee, WI 53212.

Medicare Coordinator, Alabama B/C, 450 Riverchase Parkway East, Birmingham, AL 35298.

Medicare Coordinator, Florida B/C, 532 Riverside Ave., Jacksonville, FL 32202–4918.

Medicare Coordinator, Georgia B/C, P.O. Box 9048, 2357 Warm Springs Road, Columbus, GA 31908.

Medicare Coordinator, Mississippi B/C □ MS, P.O. Box 23035, 3545 Lakeland Drive, Jackson, MI 39225–3035.

Medicare Coordinator, North Carolina B/C, P.O. Box 2291, Durham, NC 27702–2291.

Medicare Coordinator, Palmetto GBA A/ RHHI, 17 Technology Circle, Columbia, SC 29203–0001.

Medicare Coordinator, Tennessee B/C, 801 Pine Street, Chattanooga, TN 37402–2555.

Medicare Coordinator, Anthem Insurance Co. (Anthm In), P.O. Box 50451, 8115 Knue Road, Indianapolis, IN 46250–1936.

Medicare Coordinator, Arkansas B/C, 601 Gaines Street, Little Rock, AR 72203.

Medicare Coordinator, Group Health of Oklahoma, 1215 South Boulder, Tulsa, OK 74119–2827.

Medicare Coordinator, TrailBlazer, P.O. Box 660156, Dallas, TX 75266–0156.

Medicare Coordinator, Cahaba GBA, Station 7, 636 Grand Avenue, Des Moines, IA 50309–2551.

Medicare Coordinator, Kansas B/C, P.O. Box 239, 1133 Topeka Ave., Topeka, KS 66629–0001.

Medicare Coordinator, Nebraska B/C, P.O. BOX 3248, Main PO Station, Omaha, NE 68180–0001.

Medicare Coordinator, Mutual of Omaha, P.O. Box 1602, Omaha, NE 68101.

Medicare Coordinator, Montana B/C, P.O. Box 5017, Great Falls Div., Great Falls, MT 59403–5017.

Medicare Coordinator, Noridian, 4510 13th Avenue S.W., Fargo, ND 58121–0001.

Medicare Coordinator, Utah B/C, P.O. Box 30270, 2455 Parleys Way, Salt Lake City, UT 84130–0270.

Medicare Coordinator, Wyoming B/C, 4000 House Avenue, Cheyenne, WY 82003.

Medicare Coordinator, Arizona B/C, P.O. Box 37700, Phoenix, AZ 85069.

Medicare Coordinator, UGS, P.O. Box 70000, Van Nuys, CA 91470–0000.

Medicare Coordinator, Regents BC, P.O. Box 8110 M/S D–4A, Portland, OR 97207–8110.

Medicare Coordinator, Premera BC, P.O. Box 2847, Seattle, WA 98111–2847.

4. Medicare Carriers

Medicare Coordinator, NHIC, 75 Sargent William Terry Drive, Hingham, MA 02044.

Medicare Coordinator, B/S Rhode Island (RI BS), 444 Westminster Street, Providence, RI 02903–2790.

Medicare Coordinator, Trailblazer Health Enterprises, Meriden Park, 538 Preston Ave., Meriden, CT 06450.

Medicare Coordinator, Upstate Medicare Division, 11 Lewis Road, Binghamton, NY 13902.

Medicare Coordinator, Empire Medicare Services, 2651 Strang Blvd., Yorktown Heights, NY, 10598.

Medicare Coordinator, Empire Medicare Services, NJ, 300 East Park Drive, Harrisburg, PA 17106.

Medicare Coordinator, Triple S, #1441 F.D., Roosvelt Ave., Guaynabo, PR 00968.

Medicare Coordinator, Group Health Inc., 4th Floor, 88 West End Avenue, New York, NY 10023.

Medicare Coordinator, Highmark, P.O. Box 89065, 1800 Center Street, Camp Hill, PA 17089–9065.

Medicare Coordinator, Trailblazers Part B, 11150 McCormick Drive, Executive Plaza 3 Suite 200, Hunt Valley, MD 21031.

Medicare Coordinator, Trailblazer Health Enterprises, Virginia, P.O. Box 26463, Richmond, VA 23261–6463. United Medicare Coordinator, Tricenturion, 1 Tower Square, Hartford, CT 06183.

Medicare Coordinator, Alabama B/S, 450 Riverchase Parkway East, Birmingham, AL 35298.

Medicare Coordinator, Cahaba GBA, 12052 Middleground Road, Suite A, Savannah, GA 31419.

Medicare Coordinator, Florida B/S, 532 Riverside Ave, Jacksonville, FL 32202–4918.

Medicare Coordinator, Administar Federal, 9901 Linnstation Road, Louisville, KY 40223.

Medicare Coordinator, Palmetto GBA, 17 Technology Circle, Columbia, SC 29203–0001.

Medicare Coordinator, CIGNA, 2 Vantage Way, Nashville, TN 37228.

Medicare Coordinator, Railroad Retirement Board, 2743 Perimeter Parkway, Building 250, Augusta, GA 30999.

Medicare Coordinator, Cahaba GBA, Jackson Miss, P.O. Box 22545, Jackson, MS 39225–2545.

Medicare Coordinator, Adminastar Federal (IN), 8115 Knue Road, Indianapolis, IN 46250–1936.

Medicare Coordinator, Wisconsin Physicians Service, P.O. Box 8190, Madison, WI 53708–8190.

Medicare Coordinator, Nationwide Mutual Insurance Co., P.O. Box 16788, 1 Nationwide Plaza, Columbus, OH 43216–6788.

Medicare Coordinator, Arkansas B/S, 601 Gaines Street, Little Rock, AR 72203.

Medicare Coordinator, Arkansas-New Mexico, 601 Gaines Street, Little Rock, AR 72203.

Medicare Coordinator, Palmetto GBA—DMERC, 17 Technology Circle, Columbia, SC 29203–0001.

Medicare Coordinator, Trailblazer Health Enterprises, 901 South Central Expressway, Richardson, TX 75080.

Medicare Coordinator, Nordian, 636 Grand Avenue, Des Moines, IA 50309–2551.

Medicare Coordinator, Kansas B/S, P.O. Box 239, 1133 Topeka Ave., Topeka, KS 66629–0001.

Medicare Coordinator, Kansas B/S—NE, P.O. Box 239, 1133 Topeka Ave., Topeka, KS 66629–0239.

Medicare Coordinator, Montana B/S, P.O. Box 4309, Helena, MT 59601.

Medicare Coordinator, Nordian, 4305 13th Avenue South, Fargo, ND 58103–3373.

Medicare Coordinator, Noridian Bcbsnd (CO), 730 N. Simms #100, Golden, CO 80401–4730.

Medicare Coordinator, Noridian Bcbsnd (WY), 4305 13th Avenue South, Fargo, ND 58103–3373.

Medicare Coordinator, Utah B/S, P.O. Box 30270, 2455 Parleys Way, Salt Lake City, UT 84130–0270.

Medicare Coordinator, Transamerica Occidental, P.O. Box 54905, Los Angeles, CA 90054–4905.

Medicare Coordinator, NHIC—California, 450 W. East Avenue, Chico, CA 95926.

Medicare Coordinator, Cigna, Suite 254, 3150 Lakeharbor, Boise, ID 83703.

Medicare Coordinator, Cigna, Suite 506, 2 Vantage Way, Nashville, TN 37228.

Payment Safeguard Contractors

Medicare Coordinator, Aspen Systems Corporation, 2277 Research Blvd., Rockville, MD 20850.

Medicare Coordinator, DynCorp Electronic Data Systems (EDS), 11710 Plaza America Drive 5400 Legacy Drive, Reston, VA 20190–6017.

Medicare Coordinator, Lifecare Management Partners Mutual of Omaha Insurance Co., 6601 Little River Turnpike, Suite 300, Mutual of Omaha Plaza, Omaha, NE 68175.

Medicare Coordinator, Reliance Safeguard Solutions, Inc., P.O. Box 30207, 400 South Salina Street, 2890 East Cottonwood Pkwy., Syracuse, NY 13202.

Medicare Coordinator, Science Applications International, Inc., 6565 Arlington Blvd. P.O. Box 100282, Falls Church, VA.

Medicare Coordinator, California Medical Review, Inc., Integriguard Division Federal Sector Civil Group, One Sansome Street, San Francisco, CA 94104–4448.

Medicare Coordinator, Computer Sciences Corporation, Suite 600, 3120 Timanus Lane, Baltimore, MD 21244.

Medicare Coordinator, Electronic Data Systems (EDS), 11710 Plaza America Drive, 5400 Legacy Drive, Plano, TX 75204.

Medicare Coordinator, TriCenturion, L.L.C., P.O. Box 10028.

[FR Doc. 02–1527 Filed 1–22–02; 8:45 am]

BILLING CODE 4120–03–U

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Proposed Information Collection Activity; Comment Request

Proposed Projects

Title: Child and Family Services Plan, Annual Progress and Services Report, and Budget Request.

OMB No.: 0980–0047.

Description: Under title IV–B, subparts 1 and 2, of the Social Security Act, States and Indian Tribes are to submit a five year Child and Family Services Plan, an Annual Progress and Services Report (APSR), and an annual budget request and estimated expenditure report (CFS–101). The plan is used by States and Indian Tribes to develop and implement services, and describe coordination efforts with other Federal, state and local programs. The APSR is used to provide updates and changes in the goals and services under the five year plan. The CFS–101 will be submitted annually with the APSR to apply for appropriated funds for the next fiscal year. The CFSP also includes the required State plans under seciton 106 of the Child Abuse Prevention Treatment Act and section 477 of title IV–E, the Chafee Foster Care Independence Program.

Respondents: 300.

ANNUAL BURDEN ESTIMATES

Instrument	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
CFSP	300	1	500	30,000
APSR	300	1	270	81,000
CFS–101	300	1	5	1,500
Estimated total annual burden hours				112,500