FEDERAL RESERVE SYSTEM

Change in Bank Control Notices; Acquisition of Shares of Bank or Bank Holding Companies

The notificants listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the office of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received not later than November 21, 2006.

A. Federal Reserve Bank of Chicago (Patrick M. Wilder, Assistant Vice President) 230 South LaSalle Street, Chicago, Illinois 60690-1414:

1. David R. Barnes and Francesca DeRose, both of Racine, Wisconsin; Nicolet DeRose, Kenosha, Wisconsin, and Kari Barnes, Tigard, Oregon; to acquire voting shares of Wisconsin Bancshares, Inc., Kenosha, Wisconsin, and thereby indirectly acquire voting shares of Banks of Wisconsin, Kenosha, Wisconsin.

B. Federal Reserve Bank of Minneapolis (Jacqueline G. King, Community Affairs Officer) 90 Hennepin Avenue, Minneapolis, Minnesota 55480-0291:

1. Karen K. Zaun, Saint Cloud, Minnesota; to acquire voting shares of Eden Valley Bancshares, Inc., Eden Valley, Minnesota, and thereby indirectly acquire voting shares of State Bank in Eden Valley, Eden Valley, Minnesota.

Board of Governors of the Federal Reserve System, November 1, 2006.

Jennifer J. Johnson,

Secretary of the Board.

[FR Doc. E6–18621 Filed 11–3–06; 8:45 am]

BILLING CODE 6210–01–S

FEDERAL RESERVE SYSTEM

Formations of, Acquisitions by, and Mergers of Bank Holding Companies

The companies listed in this notice have applied to the Board for approval, pursuant to the Bank Holding Company Act of 1956 (12 U.S.C. 1841 *et seq.*) (BHC Act), Regulation Y (12 CFR Part 225), and all other applicable statutes and regulations to become a bank holding company and/or to acquire the assets or the ownership of, control of, or the power to vote shares of a bank or bank holding company and all of the banks and nonbanking companies owned by the bank holding company, including the companies listed below.

The applications listed below, as well as other related filings required by the Board, are available for immediate inspection at the Federal Reserve Bank indicated. The application also will be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing on the standards enumerated in the BHC Act (12 U.S.C. 1842(c)). If the proposal also involves the acquisition of a nonbanking company, the review also includes whether the acquisition of the nonbanking company complies with the standards in section 4 of the BHC Act (12 U.S.C. 1843). Unless otherwise noted, nonbanking activities will be conducted throughout the United States. Additional information on all bank holding companies may be obtained from the National Information Center Web site at http://www.ffiec.gov/nic/.

Unless otherwise noted, comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors not later than December 1, 2006.

A. Federal Reserve Bank of St. Louis (Glenda Wilson, Community Affairs Officer) 411 Locust Street, St. Louis, Missouri 63166-2034:

1. The McGehee Bank Employee Stock Ownership Plan, McGehee, Arkansas; to become a bank holding company by acquiring up to 28 percent of the voting shares of Southeast Financial Bankstock Corporation, McGehee, Arkansas, and thereby indirectly acquire voting shares of McGehee Bank, McGehee, Arkansas.

Board of Governors of the Federal Reserve System, November 1, 2006.

Jennifer J. Johnson,

Secretary of the Board.

[FR Doc. E6–18622 Filed 11–3–06; 8:45 am]

BILLING CODE 6210–01–S

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers For Medicare & Medicaid Services

Privacy Act of 1974; Report of a Modified or Altered System

AGENCY: Centers for Medicare & Medicaid Services, HHS.

ACTION: Notice of a 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 an existing system of records titled ''Common Working File (CWF),'' System No. 09–70–0526,'' most recently modified at 67 **Federal Register** (FR) 3210 (January 23, 2002). We propose to modify existing routine use number 1 that permits disclosure to agency contractors and consultants to include disclosure to CMS grantees who perform a task for the agency. CMS grantees, charged with completing projects or activities that require CMS data to carry out that activity, are classified separate from CMS contractors and/or consultants. The modified routine use will remain as routine use number 1.

We will delete routine use number 8 authorizing disclosure to support constituent requests made to a congressional representative. If an authorization for the disclosure has been obtained from the data subject, then no routine use is needed. The Privacy Act allows for disclosures with the ''prior written consent'' of the data subject. We will modify existing routine use number 5 that permits disclosure to Peer Review Organizations (PRO). Organizations previously referred to as PROs will be renamed to read: Quality Improvement Organizations (QIO). Information will be disclosed to QIOs relating to assessing and improving quality of care as well as proper payment of claims. The modified routine use will remain as routine use number 5. We will broaden the scope of routine uses number 10 and 11, authorizing disclosures to combat fraud and abuse in the Medicare and Medicaid programs to include combating ''waste'' which refers to specific beneficiary/recipient practices that result in unnecessary cost to all Federally-funded health benefit programs.

We are modifying the language in the remaining routine uses to provide a proper explanation as to the need for the routine use and 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 or because of the impact of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Public Law 108–173) provisions and to update language in the administrative sections to

correspond with language used in other CMS SORs.

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: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or grantee; (2) assist another Federal or State agency, agency of a State government, an agency established by State law, or its fiscal agent; (3) assist third party contacts; (4) assist providers and suppliers of services directly or through fiscal intermediaries or carriers; (5) support Quality Improvement Organizations (QIO) or Quality Review Organizations; (6) assist insurance companies and other groups providing protection for their enrollees, or who are primary payers to Medicare in accordance with 42 United States Code (U.S.C.) 1395y (b); (7) support an individual or organization for research, evaluation, or epidemiological projects; (8) support litigation involving the Agency related to this system of records; and (9) combat fraud, waste, 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 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 Homeland Security & Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on 10/30/2006. To ensure that all parties have adequate time in which to comment, the modified system, including routine uses, will become effective 30 days from the publication of the notice, or 40 days from the date it was submitted to OMB and Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: CMS Privacy Officer, Division of Privacy Compliance, Enterprise Architecture and Strategy Group, Office of Information Services, 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 Systems Operations, Business Applications Management Group, Office of Information Services, CMS, Room N2–08–18, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–6160.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified or Altered System of Records

A. Statutory and Regulatory Basis for 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 U.S.C. 1395h, and 1395kk).

B. Collection and Maintenance of Data in 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. 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.

II. Agency Policies, Procedures, and Restrictions on The Routine Use

A. 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 Disclosures of Data in the System.'' Both identifiable and non-identifiable data may be disclosed under a routine use.

We will only collect 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. Disclosure of information from this system will be approved only to the extent necessary to accomplish the purpose of the disclosure and 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 potential 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; and

b. remove or destroy at the earliest time all patient-identifiable information.

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, consultants, or grantees, who have been engaged by the agency to assist in the performance of a service related to this collection and who need to have access to the records in order to perform the activity.

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 CMS function relating to purposes for this system.

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, consultant or grantee 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, consultant or grantee from using or disclosing the information for any purpose other than that described in the contract and requires the contractor, consultant or grantee 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 United States Postal Service may require CWF data for investigating alleged forgery or theft of reimbursement checks.

The Railroad Retirement Board 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 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, waste, 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 clearinghouses, 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 Quality Improvement Organizations (QIO) in connection with review of claims, or in connection with studies or other review activities, conducted pursuant to Part A and 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.

QIOs will work to implement quality improvement programs, provide consultation to CMS, its contractors, and to State agencies. QIOs will assist the State agencies in related monitoring and enforcement efforts, assist CMS and Intermediaries and Carriers 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.

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 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.

9. 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, waste, 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, waste, or 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.

10. 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, waste, 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, waste, and abuse in such Federally-funded programs.

B. Additional Circumstances Affecting Routine Use Disclosures

To the extent this system contains Protected Health Information (PHI) as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, Subparts A and E) 65 FR 82462 (12–28–00). Disclosures of such PHI that are otherwise 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.'' (See 45 CFR 164–512 (a) (1)).

In addition, our policy will be to prohibit release even of data not directly identifiable, except pursuant to one of the routine uses or if required by law, if we determine 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 could, because of the small size, use this information to deduce the identity of the beneficiary).

IV. Safeguards

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: The Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E–Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

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

CMS proposes to modify 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 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 of patients whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure from the proposed 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 information relating to individuals.

Dated: October 24, 2006.

John R. Dyer,

Chief Operating Officer, Centers for Medicare & Medicaid Services.

System No. 09–70–0526

SYSTEM NAME:

• Common Working File (CWF),'' HHS/CMS/OIS.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

The Centers for Medicare & Medicaid Services (CMS) Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850 and at CMS Host Sites located in Birmingham, Alabama, and Dallas, Texas.

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 (U.S.C.) 1395h, and 1395kk).

PURPOSE(S) OF THE SYSTEM:

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: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or grantee; (2) assist another Federal or State agency, agency of a State government, an agency established by State law, or its fiscal agent; (3) assist third party contacts; (4) assist providers and suppliers of services directly or through fiscal intermediaries or carriers; (5) support Quality Improvement Organizations (QIO) or Quality Review Organizations; (6) assist 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); (7) support an individual or organization for research, evaluation, or epidemiological projects; (8) support litigation involving the Agency related to this system of records; and (9) combat fraud, waste, 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:

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, consultants, or grantees, who have been engaged by the agency to assist in the performance

of a service related to this collection and who need to have access to the records in order to perform the activity.

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 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, waste, 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 Quality Improvement Organizations (QIO) in connection with review of claims, or in connection with studies or other review activities, conducted pursuant to Part A and 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 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.

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 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.

9. 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, waste, or abuse in such program.

10. 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, waste, 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, waste, or abuse in such programs.

B. Additional Circumstances Affecting Routine Use Disclosures

To the extent this system contains Protected Health Information (PHI) as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, Subparts A and E) 65 **Federal Register** 82462 (12–28–00). Disclosures of such PHI that are otherwise 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.'' (See 45 CFR 164–512(a)(1)).

In addition, our policy will be to prohibit release even of data not directly identifiable, except pursuant to one of the routine uses or if required by law, if we determine 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 could, because of the small size, use this information to deduce the identity of the beneficiary).

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 in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

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, then destroyed 6 years and 3 months after final payment/action. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER AND ADDRESS:

Director, Division of Systems Operations, Business Applications Management Group, Office of Information Services, CMS, Room N2–08–18, 7500 Security Boulevard, 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, assigned card key number, and building/secure area, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and 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 specify the record contents being sought. (These procedures are in accordance with department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORDS PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the records 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).

RECORDS 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.

[FR Doc. E6–18611 Filed 11–3–06; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers For Medicare & Medicaid Services

Privacy Act of 1974; Report of a Modified or Altered System of Records

AGENCY: Centers for Medicare & Medicaid Services, HHS.

ACTION: Notice of a modified or altered system of records (SOR).

SUMMARY: In accordance with the Privacy Act of 1974, we are proposing to modify or alter an existing SOR, ''Intermediary Medicare Claims Record (IMCR) System,'' System No. 09–70–0503, last published at 67 **Federal Register** 65982 (October 29, 2002). We propose to change the name of this system to more closely reflect the name of the program used for the processing of Part A claims. We will modify the name to read: ''Fiscal Intermediary Shared System (FISS).'' We propose to modify existing routine use number 1 that permits disclosure to agency contractors and consultants to include disclosure to CMS grantees who perform a task for the agency. CMS grantees, charged with completing projects or activities that require CMS data to carry out that activity, are classified separate from CMS contractors and/or consultants. The modified routine use will remain as routine use number 1. We will delete routine use number 8 authorizing disclosure to support constituent requests made to a congressional representative. If an authorization for the disclosure has been obtained from the data subject, then no routine use is needed. The Privacy Act allows for disclosures with the ''prior written consent'' of the data subject. We will broaden the scope of routine uses number 10 and 11, authorizing disclosures to combat fraud and abuse in the Medicare and Medicaid programs to include combating ''waste'' which refers to specific beneficiary/recipient practices that result in unnecessary cost to all Federally-funded health benefit programs.

We are modifying the language in the remaining routine uses to provide a proper explanation as to the need for the routine use and 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 or because of the