Program Memorandum Intermediaries/Carriers

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

Transmittal AB-03-034 **Date: FEBRUARY 28, 2003**

CHANGE REQUEST 2484

SUBJECT: Medicare Fee for Service Contractor Guidance on the HIPAA Privacy Rule

The purpose of this Program Memorandum (PM) is to provide guidance in describing the roles of Medicare FFS contractors (i.e., fiscal intermediaries, carriers, DMERC and Program Safeguard Contractors) and the Centers for Medicare & Medicaid Services (CMS) in implementing the "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") for the Original Medicare ("Original Medicare") Fee-For-Service (FFS) Health Plan. This guidance summarizes the operational activities that are being developed to ensure Original Medicare's compliance with the Privacy Rule by the April 14, 2003 compliance date required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Privacy Rule applies to three types of entities, which collectively are termed "covered entities" and are subject to the requirements of HIPAA. The covered entities are health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically.

The Privacy Rule applies to Original Medicare, which under the Rule is a health plan and therefore a "covered entity." CMS is responsible for ensuring that Medicare complies with the privacy standards.

The Privacy Rule is based on the same fair information principles that are found in the Privacy Act of 1974, and are now generally extended to the public and private sectors of the health care delivery system. The Privacy Rule applies to protected health information as defined by the Rule while the Privacy Act protects records with individually identifiable information held by Federal agencies. The Privacy Act continues to apply to Medicare and Medicare FFS contractors in their day-to-day operations.

In addition to the summary, CMS has developed a list of questions and answers that follow. They are available from the CMS Web site at http://cms.hhs.gov/contractors/.

Privacy Rule Requirements

The Department of Health and Human Services (HHS) issued the Privacy Rule (45 CFR Parts 160 and 164, 65 Federal Register 82462 as amended by 66 FR 12434). The HHS Office for Civil Rights (OCR) is responsible for providing outreach and technical assistance to covered entities and for enforcement. The OCR maintains information on the Privacy Rule at http://www.hhs.gov/ocr/hipaa/, including Frequently Asked Questions.

Listed below is a brief description of the Privacy Rule requirements, how the requirements apply to Medicare, and how CMS central office is operationalizing them.

Business Associates

Most health care providers and health plans do not carry out all of their health care activities and functions by themselves; they require assistance from a variety of contractors and other businesses. The Privacy Rule allows providers and plans to give protected health information (PHI) to their "business associates" as long as they have satisfactory assurances and document those assurances, typically by contract, that business associates will safeguard the information.

The privacy modifications issued by HHS on August 14, 2002, (67 Federal Register 53182) contain Sample Business Associate Contract Provisions that covered entities may use. Covered entities may have up to an additional year to change existing written contracts to come into compliance with business associate requirements, that is, by April 14, 2004.

As a Medicare contractor that participates in FFS claims processing, you are a business associate of the Original Medicare plan. When your Medicare contract is modified, the business associate provisions will be added. These provisions will also address your responsibility to ensure that your subcontractors or agents to whom you disclose Medicare data agree, by contract, to safeguard any PHI as well. Your contract will continue to include language that applies to contractors who maintain or operate a Privacy Act protected systems of records on Medicare's behalf.

Notice of Privacy Practices

The Privacy Rule requires each covered entity to develop and provide a plain language notice that describes its legal duties, the uses and disclosures of protected health information that it may make, and individual rights and how to exercise them.

Since CMS is responsible for Original Medicare, CMS developed a Notice of Privacy Practices, effective on April 14, 2003, for Medicare beneficiaries. Medicare's privacy notice was provided to beneficiaries for the first time in the 2003 *Medicare & You* handbook that was mailed beginning in October 2002. New enrollees will receive the privacy notice when the handbook is mailed (within 30 days of Medicare entitlement).

Since Medicare's privacy notice describes the uses and disclosures of PHI in the day-to-day operations of Medicare (including Medicare FFS contractors), you are **not** to develop a separate privacy notice for Medicare beneficiaries.

Authorization

The Privacy Rule requires an individual's written authorization in order for a covered entity to use or disclose PHI for purposes other than treatment, payment, or health care operations.

CMS is developing a model authorization for beneficiaries or their personal representatives to request disclosure of PHI to third parties. The model will contain the elements for compliance with both the Privacy Rule and Privacy Act requirements. As soon as the model authorization form is available, it will be shared with our contractors. Until then, continue to use authorizations under existing customer service procedures.

Opportunity to Agree/Object

The Privacy Rule permits covered entities to disclose PHI to persons who are family members or relatives of, or other persons identified by, the individual, and are currently involved in the individual's health care or payment for health care. Covered entities may disclose PHI when the individual is present and agrees to the disclosure being made to the person involved in his or her health care.

You may continue to handle routine inquiries, such as telephone requests for the status of claims, under existing customer service procedures that include verification of the individual's identity. Therefore, with the beneficiary's verbal or written permission, you may continue to speak with third parties on behalf of the individual. Refer to Change Request 2237, Transmittal AB-02-094, dated July 3, 2002, for instructions on disclosing individually identifiable information over the phone.

You may also continue to handle Congressional inquiries under existing customer service procedures that include verification of the individual's identity and authority.

Individual Rights and Complaints

The Privacy Rule gives individuals rights with respect to their PHI. These rights are listed in the covered entities' privacy notices, and include the right to inspect, copy, and amend the individual's PHI, the right to request restrictions, confidential communications, accounting of disclosures, paper copy of privacy notice, and filing complaints.

Medicare's Notice of Privacy Practices informs beneficiaries who are interested in exercising individual rights and filing complaints to go to www.medicare.gov or call 1-800-MEDICARE (1-800-633-4227). The Web site and Customer Service Representatives at 1-800 MEDICARE will provide information on how to exercise individual rights and file complaints.

Medicare is establishing a centralized process by April 14, 2003, to respond to beneficiary requests to exercise individual rights and to complain. If procedures are in place prior to the effective date, central office will respond to written requests and complaints. Central office is establishing a process to be able to respond to requests specific to the Privacy Rule by April 14, 2003. Requests that fall under the Privacy Act or other existing information authority will continue to be processed according to existing procedures.

We do not anticipate that our Medicare FFS contractors will be responding to beneficiary requests to exercise individual rights and filing complaints. Your role is limited to referring beneficiary inquiries and complaints to central office.

Administrative Requirements

As Medicare's business associate, you are not subject to the administrative requirements of the Privacy Rule (but business associates may also be covered entities in their own right and therefore subject to the Rule's requirements). However, under the Privacy Act, you are Medicare's agent and therefore must comply with the privacy provisions specified in your contract.

Compliance Date

Covered entities, including the original Medicare plan, are required to be in compliance with the provisions of the Privacy Rule by April 14, 2003 (April 14, 2004, for small health plans). The Administrative Simplification Compliance Act (ASCA) does not affect the Privacy Rule's compliance. The ASCA instead enabled covered entities other than small health plans, (which already had the later compliance date), to obtain a one-year delay in the date on which they must comply with the requirements of the Transactions Rule, or the "Standards for Electronic Transactions" (published on August 17, 2000). For those entities that obtained an extension under ASCA, their new compliance date is October 16, 2003.

The *effective date* for this PM is April 14, 2003.

The *implementation date* for this PM is April 14, 2003.

These instructions should be implemented within your current operating budget.

This PM may be discarded after January 30, 2004.

If you have any questions concerning privacy policy, contact Robin Getzendanner at rgetzendanner@cms.hhs.gov or call 410-786-9621. For other contractor related questions contact Verne Rinker at vrinker@cms.hhs.gov or call 410-786-8867.

Attachment

ATTACHMENT

COVERED ENTITY

Question: Is CMS a "covered entity" under HIPAA?

Answer: The Federal health programs that CMS administers are health plans, as defined in HIPAA, and therefore covered entities subject to the Privacy Rule. The health plans are:

- Part A or Part B of the Medicare program under Title XVIII;
- Medicaid program under Title XIX;
- State Children's Health Insurance Program (SCHIP); and
- Medicare+Choice (M+C) program and other Medicare health plans.

CMS is directly responsible for ensuring that the Medicare Fee-For-Service (FFS) program, also known as the Original Medicare Plan, complies with the Privacy Rule by the April 14, 2003 compliance date. For the Medicaid and SCHIP programs, the appropriate State Agency is responsible for ensuring compliance with privacy requirements. M+C plans are covered entities subject to the Privacy Rule in their own right and responsible for their own compliance.

BUSINESS ASSOCIATES

Question: Are Medicare Fee-For-Service contractors (i.e., intermediaries, carriers, DMERC and program safeguard contractors) considered business associates of Medicare (the covered entity)?

Answer: Medicare FFS contractors are business associates of Medicare under the Privacy Rule.

Question: As business associates of Medicare, will Medicare FFS contractors be required to execute a HIPAA business associate contract with CMS? If so, will the business associate contract require that Medicare FFS contractors sign HIPAA-compliant "business associate" agreements with all subcontractors of Medicare FFS contractors? Will CMS provide a "model" contract for this purpose or can Medicare FFS contractors use their own corporate business associate agreements for subcontracts?

Answer: Your contract with CMS will be modified the earlier of the date the contract is up for renewal or April 14, 2004. The contract and any subcontracts that you have must include specific subsections in the *Appendix to the Preamble - Sample Business Associate Contract* published in the modifications to the HIPAA Privacy Final Rule (FR Vol. 67, No. 157, p. 53264, dated 8/14/02). These provisions address your responsibility to ensure that your subcontractors or agents to whom you disclose Medicare data agree, by contract, to safeguard all protected health information.

Your contract will continue to include language that applies to contractors who maintain or operate a Privacy Act protected Systems of Records on CMS behalf.

Question: Does the 1-year extension for ***existing*** contracts provide an additional 1-year (i.e., April 2004) for Medicare FFS contractors to update the contract with CMS and all subcontracts?

Answer: Not exactly. The Final Privacy Rule, as amended, provides that prior contracts and subcontracts shall be "deemed" compliant until the earlier of April 14, 2004 or the date such contract is renewed or modified after the compliance date of April 14, 2003.

Question: If Medicare is doing a common audit for a State Medicaid Agency, will the Program Safeguard Contractor (PSC) need a business associate contract with the State Agency?

Answer: Yes. The PSC will need a business associate contract with that state agency whenever there is the likelihood that the PSC would be handling protected health information during the course of the audit.

Question: Are physicians or other providers considered business associates of a health plan or other payer?

Answer: This question is answered in the Frequently Asked Questions (FAQ), published by OCR on October 2, 2002. It states, "Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. A business associate relationship could arise if the provider is performing a function on behalf of, or providing services to, the health plan (e.g. case management services). See the discussion at 67 Fed. Reg. 14776, 14788 (March 27, 2002) concerning this issue."

CMS PRIVACY RULE IMPLEMENTATION

Question: What has CMS done to implement the Privacy Rule?

Answer: To ensure Medicare's compliance by April 14, 2003, CMS developed and implemented a 3-phased plan that was approved by the Agency's Beneficiary Confidentiality Board (BCB). The BCB has executive oversight of CMS's privacy implementation plan as well as for the ongoing compliance program to ensure continued adherence to privacy requirements.

The Agency-wide plan was implemented in June 2001 and includes the following phases:

- Identifying agency activities subject to privacy requirements;
- Baseline assessment and gap analysis; and
- Workplan, implementation, and verification.

CMS's identification of its business functions subject to privacy requirements and assessment of gaps were very useful in planning for agency-wide compliance with new privacy standards (e.g., Notice of Privacy Practices, authorizations).

Question: As business associates of Medicare, can you clarify what the expectations of Medicare FFS contractors are going to be with respect to conducting a privacy assessment?

Answer: Currently, under the Privacy Act, you only use that information which is necessary to carry out the work of the Medicare program. There is no new requirement to perform assessments of uses, disclosures or minimum necessary requirements under the Privacy Rule.

BUDGET

Question: Will HIPAA privacy activities of Medicare FFS contractors be funded?

Answer: No additional funding will be provided by CMS; contractor activities are to be carried out within the FY03 operating budget.

Question: Will the HIPAA privacy regulations necessitate system changes?

Answer: No new systems changes are required by these instructions.

NOTICE OF PRIVACY PRACTICES

Question: As "individuals", Medicare beneficiaries are entitled to receive a Notice of Privacy Practices. Who will issue the notice and when will it be distributed?

Answer: CMS developed a Notice of Privacy Practices, effective on April 14, 2003, for Medicare beneficiaries. Since Medicare's privacy notice describes the uses and disclosures of individually identifiable information in the day-to-day operations of Medicare and its contractors, you are **not** to develop a separate privacy notice for Medicare beneficiaries.

Medicare's Notice of Privacy Practices was provided to beneficiaries for the first time in the 2003 *Medicare & You* handbook that was mailed to beneficiaries beginning in October 2002. New enrollees will receive the privacy notice when the handbook is mailed (within 30 days of Medicare entitlement).

Question: When a beneficiary calls a contractor and wants a copy of the Notice of Privacy Practices, what action should the contractor take?

Answer: You can tell beneficiaries that their copy of Medicare's privacy notice is in their 2003 *Medicare & You* handbook on pages 50-53, and is also posted on Medicare's Web site at www.medicare.gov.

Question: How will a Medicare beneficiary know how to exercise his/her individual rights identified in the Notice of Privacy Practices?

Answer: Medicare's Notice of Privacy Practices informs beneficiaries who are interested in exercising individual rights to go to www.medicare.gov or call 1-800-MEDICARE. Customer Service Representatives (CSR) at 1-800-MEDICARE will have scripts to answer questions regarding exercising individual rights and filing complaints.

Question: How will Medicare handle a beneficiary's request to exercise his/her individual rights under the Privacy Rule?

Answer: The individual rights include the right to inspect and copy protected health information, amend protected health information, the right to request restrictions, confidential communications, accounting of disclosures, a paper copy of the privacy notice, and how to file complaints.

CMS is responsible for responding to beneficiary inquiries about individual rights. CMS is establishing a centralized process using existing customer service resources. This integrated operation will enable Medicare to respond to written beneficiary inquiries on individual rights (and also handle complaints) by April 14, 2003. If procedures are in place prior to the compliance date, central office will respond to written inquiries and complaints. Where procedures are still being developed, central office will send a written acknowledgement that the inquiry/complaint cannot be processed at the present time and that a response will be sent on or shortly after April 14, 2003.

We do not anticipate that our Medicare FFS contractors will be responding to beneficiary inquiries on individual rights and complaints. Your role is limited to referring beneficiary inquiries and complaints to central office.

If you receive a request from a beneficiary **explicitly wishing to exercise his/her individual rights under the Privacy Rule**, advise him or her to send a written request to (or forward it if you receive a written request):

HIPAA Privacy
P.O. Box 8050
U. S. Department of Health and Human Services
Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Process requests that are not explicitly Privacy Rule requests according to the current procedures outlined below.

ACCESS & AMENDMENT

Question: Will CMS or the contractors provide beneficiary access under the Privacy Rule?

Answer: CMS is responsible for responding to beneficiary requests for access to records under the Privacy Rule. Medicare FFS contractors should only respond to those requests for information related to payment of a claim, for which you are already responsible under the contract under existing customer service procedures.

Question: Please explain the relationship between requests for access under the Freedom of Information Act (FOIA), the Privacy Act of 1974, and the Privacy Rule, including the timeliness standards.

Answer: CMS provides numerous individuals and organizations access to a broad array of information under many statutes, including FOIA and the Privacy Act. FOIA and Privacy Act requests will continue to be handled according to current procedures and timeliness standards. A FOIA request for access to public records requires CMS, as a Federal Agency, to provide the fullest possible disclosure of its records to the public, subject to certain exceptions (e.g., proprietary information, national defense risks). The Privacy Act requires CMS to provide access for individuals to their personal information maintained in a System of Records. Note that an individual's request under the Privacy Act to access his or her records must specify a Privacy Act System of Records and must be addressed to the system manager identified in the **Federal Register** notice.

A Privacy Rule request for access is separate from both FOIA and the Privacy Act and has it own timeliness standards associated with it. Requests for access under the Privacy Rule will be handled through CMS' centralized process.

Question: Are simple telephone inquiries, such as asking about the status of a claim or requesting a duplicate Medicare Summary Notice, considered a HIPAA request for access?

Answer: No. You should continue to handle routine inquiries under existing customer service procedures.

Question: Will contractors be responsible for amendments to beneficiary records?

Answer: No. CMS is responsible for handling beneficiary requests to amend the record under the Privacy Rule. This is part of the centralized process being developed and implemented to respond to beneficiaries' requests regarding individual rights. Therefore, you will not be responding to requests to amend records.

Only a request from a beneficiary that **explicitly states that he/she wishes to exercise his/her individual rights under the Privacy Rule** will be handled through the centralized process. Other requests for changes to claims or payment records, such as an appeal or change of address request, are not considered Privacy Rule requests for amendments, and should be handled according to current procedures.

Please note, however, that if the request for amendment involves medical records, you should explain that, except in rare circumstances, only the source of the medical record (i.e., the provider) may make changes to the record.

ACCOUNTING FOR DISCLOSURES

Question: Do Medicare FFS contractors have to account for disclosures under the Privacy Rule?

Answer: No. Under the Privacy Act, you are only allowed to use individually identifiable information in the course of your Medicare business. In June 2000, CMS issued CR 1156, Transmittal AB-00-46 entitled, *HCFA Policy for Disclosure of Individually Identifiable Information*. Those instructions state that any disclosure of individually identifiable information without prior consent from the individual to whom the information pertains, or without statutory or contract authorization, requires CMS' prior approval. CMS uses Data Use Agreements to track all

disclosures that are authorized by CMS (e.g., General Accounting Office, OIG [Office of Inspector General]).

CMS is responsible for responding to beneficiary requests on accounting of disclosures under the Privacy Rule. This is part of the centralized process being developed and implemented to respond to beneficiaries on individual rights. Therefore, you will not be responding to requests for an accounting of disclosures.

Question: Is it a disclosure when a Medicare FFS contractor provides claims files to the Office of the Inspector General (OIG) for audit sampling purposes?

Answer: Yes. The Privacy Rule would consider these to be disclosures by a business associate of the covered entity. The disclosures though are permissible under several avenues: as health care operations, as required by law, or as required for the investigation and prevention of fraud and abuse. Note that disclosures for health care operations are not required to be included in any accounting of disclosures.

RIGHT TO RESTRICT/CONFIDENTIAL COMMUNICATIONS

Question: Will Medicare FFS contractors be responsible for responding to requests to restrict the use of an individual's protected health information?

Answer: CMS is responsible for responding to beneficiary requests to restrict. This is part of the centralized process being developed and implemented to respond to beneficiaries on individual rights. Therefore, you will not be responding to requests to restrict.

Question: Will Medicare FFS contractors be responsible for responding to requests for confidential communications?

Answer: Current regulations and existing agreements with the Social Security Administration are extremely prescriptive, often governing precisely how CMS can respond to requests for confidential communications.

Operationally, we can only maintain one address at a time. Because of this, routine change of address requests should be handled according to current change of address procedures. Follow instructions found at Part 3, §7009 of the Medicare Carrier Manual or Part 3, §3717.1 of the Medicare Intermediary Manual entitled *Beneficiary Address Change* to carry out routine requests for change of address.

COMPLAINTS

Question: Will contractors handle complaints about privacy violations at the contractor level or will they be handled by CMS?

Answer: Medicare's Notice of Privacy Practices informs individuals of the right to file complaints about Medicare's privacy practices with either Medicare or the Secretary of Health and Human Services. The privacy notice refers individuals to www.medicare.gov or 1-800-MEDICARE for further information on filing a complaint.

If you receive a complaint from an individual concerning Medicare's privacy practices, advise him or her to send a written complaint to (or forward it if you receive a written request):

Privacy Complaints
P.O. Box 8050
U. S. Department of Health and Human Services
Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Central office is responsible for maintaining a record of complaints and their resolutions, if any. This is part of the centralized process being developed and implemented for individual rights.

An individual also has the right to complain to the Secretary of HHS. OCR is expected to issue guidance on how an individual may submit his/her complaints to the Secretary.

AUTHORIZATIONS

Question: Under the Privacy Act of 1974, Medicare currently requires authorizations for disclosures of individually identifiable information to third parties, however, the level of detail required in the authorization under the Privacy Rule is greater. Will CMS create a blanket authorization form containing the core elements outlined in the Privacy Rule?

Answer: CMS is developing a model authorization for a beneficiary or their personal representative to use to request disclosure of their protected health information to a third party. The model will contain the elements for compliance with both the Privacy Rule and Privacy Act requirements. As soon as the model authorization form is available, it will be shared with our contractors. Until then, continue to use authorizations under existing customer service procedures.

Continue to handle routine inquiries, such as telephone requests for the status of claims, under existing customer service procedures that include verification of the individual's identity. You may continue to speak with third parties on behalf of the individual after you obtain the beneficiary's verbal or written permission. Refer to CR 2237, Transmittal AB-02-094, dated July 3, 2002, entitled *Disclosure Desk Reference for Call Centers* for instructions on disclosing individually identifiable information over the phone.

Question: Does the HIPAA Privacy Rule allow for verbal authorizations?

Answer: The Privacy Rule permits a covered entity to disclose to any person identified by the individual the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's care. Therefore, a verbal authorization is allowed under the Privacy Rule for those individuals involved in the care of an individual.

ADMINISTRATIVE REQUIREMENTS

Question: Will CMS hold contractors accountable for adhering to HIPAA privacy requirements for covered entities or for business associates?

Answer: As Medicare's business associate, you are not subject to the administrative requirements of the Privacy Rule. However, under the Privacy Act, you must comply with the privacy provisions specified in your contract.

Question: Will CMS designate a Medicare-wide privacy officer to handle privacy complaints or will each Medicare contractor need to appoint a privacy officer?

Answer: CMS has a Privacy Officer. As our business associates under the Privacy Rule, you are not required to designate a privacy official. However, your contract with CMS requires compliance with the Privacy Act and related regulations and manual instructions concerning disclosures. In June 2000, CMS issued CR 1156, Transmittal AB-00-46, entitled *HCFA Policy for Disclosure of Individually Identifiable Information*. Those instructions require you to have in place a senior official or other responsible party to address the privacy concerns of your organization and to establish an internal control system to monitor compliance with privacy requirements.

Question: Will Medicare FFS contractors be expected to do any privacy training?

Answer: The Privacy Rule requires that a covered entity train employees on its privacy policies and procedures with respect to protected health information by April 14, 2003. To comply with the training requirement, CMS employees are required to complete computer-based training on protecting the privacy and security of CMS' data.

As Medicare's business associate, you are not subject to the Privacy Rule's requirement to train your staff specifically on the Privacy Rule. However, under the Privacy Act, you are required to ensure that your employees understand their responsibility to protect the privacy and confidentiality of the Agency's records.

MISCELLANEOUS

Question: What is the relationship between the Privacy Act and the Privacy Rule?

Answer: Medicare is subject to the Privacy Act of 1974 as well as other applicable Federal statutes, regulations, instructions, and memoranda that relate to protecting individually identifiable information. Your Medicare contract requires compliance with these privacy requirements to protect the individually identifiable information that is needed to perform business functions for program administration, such as claims processing and program integrity.

In June 2000, CMS issued CR 1156, Transmittal AB-00-46, entitled *HCFA Policy for Disclosure of Individually Identifiable Information*. Those instructions enunciated the policy of CMS regarding the disclosure of individually identifiable information that is acquired and maintained under authority of Title XVIII of the Social Security Act, by Medicare fiscal intermediaries and carriers. It is CMS' policy that any data collected on behalf of CMS in the administration of your Medicare contract belongs to CMS. Any disclosure of individually identifiable information without prior consent from the individual to whom the information pertains, or without statutory or contract authorization, requires CMS' prior approval. The PM did not communicate a change, but rather a reminder of the existing policy.

Privacy provisions that currently apply to Federal Agencies under the Privacy Act are now extended through the Privacy Rule to covered entities in both the public and private sectors of the health care delivery system. The Privacy Act continues to apply to Medicare and Medicare FFS contractors. Additionally, Medicare is subject to the Privacy Rule as a health plan. As Medicare operates under both the Privacy Act and the Privacy Rule, CMS has determined how the provisions interact with each other as it uses personally identifiable information in its day-to-day operations. For example, a use or disclosure that is permitted under the Privacy Rule (e.g., to facilitate cadaveric organ donation and transplants), but not published in a Federal Register notice as a routine use in a CMS system of records would not be permitted for Medicare. We do not currently see any significant changes in the way the Medicare FFS contractors conduct Medicare business. If in the future we determine that the Privacy Rule necessitates changes in the way you do the work of the Medicare program, you will be notified.

Question: Is there any operational difference between what is protected under the Privacy Act and the Privacy Rule?

Answer: In the operation of the Medicare program, the difference between the Privacy Act and the Privacy Rule is the applicability to deceased individuals. The Privacy Act protects the identifiable information about living individuals only. Once an individual dies, his/her information is no longer protected under the Privacy Act. The Privacy Rule, however, protects protected health information (PHI) held by a covered entity regardless of whether the individual is living or deceased.

Question: The HIPAA Privacy Rule does not preempt more stringent state laws. Will contractors in such states be subject to additional privacy requirements? If so, how will those requirements be communicated, made part of contractors' work expectations, and funded? If not, what is the CMS rationale for denying additional state requirements on Medicare FFS contractors?

Answer: Medicare is a national program that is administered under Federal statute and regulation. CMS administers Medicare through our Medicare FFS contractors and you are required to operate in accordance with statutory and regulatory requirements and CMS administrative direction.

When considering the provisions of HIPAA, Congress expressly intended to defer to more stringent state laws that conflict with provisions in the Privacy Rule. The Privacy Rule therefore explicitly preempts conflicting state law provisions, unless they are more stringent or more protective of the individual's rights. Since the federal law expressly preserves more stringent state laws, and because of the complexity of this issue, you should anticipate further guidance on this from CMS as related issues arise.

Question: Do providers need to get an authorization from the beneficiary before they can share information that is needed to process the claim with the Medicare contractor?

Answer: There is no requirement to obtain an authorization from the beneficiary for treatment, payment, and health care operations. The provider should be informed that you will be unable to make payment for the claim if he/she fails to provide you the information you need to process his/her Medicare claim.

Question: Will CMS be changing any of the requirements recently issued via CR 2237 - *Disclosure Desk Reference for Call Centers*, as a result of the more stringent guidelines of HIPAA? For example, callers other than the individual that have a copy of the Explanation of Benefits (EOB) or Medicare Summary Notice (MSN) are allowed to discuss information relative to services appearing on that EOB/MSN even when an authorization has not been provided. Under HIPAA, an authorization is required when releasing PHI to other than the individual.

Answer: CMS will update CR 2237, TN AB-02-94 dated July 3, 2002, entitled *Disclosure Desk Reference for Call Centers* based on the Privacy Rule in the near future, however, we have determined that the current procedures meet the requirements of the Privacy Rule. In addition, CMS will continue to post clarifications to the call center website (http://cms.hhs.gov/callcenters/QandA.asp).

When an individual has a copy of the EOB/MSN, the Customer Service Representative (CSR) may discuss only what is on the EOB/MSN. It is not considered a disclosure if the individual already has the information. However, no additional information should be released without obtaining an authorization.

Question: The FY 2003 Budget Performance Requests (BPR) require contractors to provide CMS remote access to allow CMS personnel to hear live calls from beneficiaries to CSRs. Since beneficiaries will be discussing PHI, is this a violation of privacy regulations?

Answer: Remote access by CMS personnel is part of CMS' health care operations and therefore is not a disclosure of information and is not in violation of the privacy regulation.

Question: Must we inform the beneficiary that the contractor and CMS staff may listen to live phone calls? Please confirm if the contractors need to expand their telephone message to include that CMS may listen.

Answer: CMS is the covered entity. Contractors are business associates of CMS. Therefore remote monitoring of calls is part of CMS's healthcare operations. We believe a phrase such as, "This call may be monitored to ensure outstanding quality," will cover both the contractor and CMS staff monitoring calls.

Only CMS staff whose job description permits them to perform remote monitoring will be given access. Staff are trained to keep this information safe and secure in the same manner that confidential beneficiary information is currently safeguarded.

Question: Current instructions permit a carrier to respond to and disclose PHI to a member of Congress who is representing a beneficiary even though the carrier has no evidence from the beneficiary that the member of Congress has been appointed as his/her Personal Representative. Will this practice be changed?

Answer: You may continue to handle Congressional inquiries under existing customer service procedures that include verification of the individual's identity.

Question: What is the status of the trading partner agreement between Medicare FFS contractors and COB insurers? When can we look to receive the language and the instructions?

Answer: Currently, we are seeking Office of General Counsel's (OGC) opinion on a few issues that will influence our ability to issue the standard trading partner agreement, but we remain confident that these will be addressed before the end of the calendar year (CY) 2002. In the interim, our Medicare FFS contractors have been instructed in CR 2216, Transmittal AB-02-095, dated 7/5/02, entitled *Prohibition on New Trading Partner Agreements (TPAs) with Certain Entities for the Purpose of Coordination of Benefits (COB)* regarding what steps they may take regarding their existing agreements with non-insurers, e.g., healthcare clearinghouses, or third party administrators. The standard trading partner agreement for the purpose of COB is not designed to be a business associate agreement nor is it to be regarded as a document that will subsume all previously developed EDI agreements (also generically termed " trading partner agreements).

Question: Will the trading partner agreement be finalized by April 2003?

Answer: The Division of Benefits has every intention of issuing its standard trading partner agreement for the purpose of Coordination of Benefits before the April 14, 2003 compliance date for the Privacy Rule. Once issued, Medicare FFS contractors may begin to use this document for the purpose of entering into agreements for COB purposes with Medigap insurers, other supplemental insurers/employers retiree health plans, multiple welfare trusts, self-insured plans, State Medicaid Agencies, other Federal payers, and related entities.

Question: Currently, contractors are required to send EDI billers an EDI enrollment form for Medicare Electronic Medical Claims (EMC) submissions. Would the EMC submission process require a business associate contract between the contractor and the provider? If a business associate contract is not appropriate, will contractors be required to update the EDI enrollment form as a result of HIPAA Privacy?

Answer: HIPAA's Administrative Simplification provisions require the Secretary to adopt standards for electronic health care transactions.

The CMS Standard EDI Enrollment Form must be completed prior to submitting electronic media claims to Medicare. Completing the form constitutes an agreement between the provider and Medicare. The purpose of the agreement is to ensure that the provider understands the appropriate uses and disclosures of Medicare beneficiaries' individually identifiable information.

The relationship between a provider and Medicare is that of two covered entities sharing information for the purposes of treatment, payment, and health care operations. It is not a business associate relationship since neither entity is doing work on behalf of the other. The privacy modifications specifically allow for the sharing of information between two covered entities provided that both entities have or have had a relationship with the individual.

The Privacy Rule does not require the EDI form to be updated.