

#### d. Administrative Data Standards

As covered entities, endorsed sponsors must comply with any applicable standards, implementation specifications, and requirements set forth in 45 CFR part 162, subparts I *et seq.*, when conducting a transaction (as that term is defined under section 1173 (a) of the Act and 45 CFR 160.103) as of the compliance date of a final rule issued under that Part. In addition, such sponsors are business associates of the Medicare program (a health plan covered entity), as they perform certain administrative functions related to transitional assistance on our behalf. We will, therefore, require in our contracts with endorsed sponsors that, when conducting all or part of a transaction on our behalf, they comply with, and require their agents and subcontractors to comply with, all requirements under 45 CFR part 162 applicable to CMS as a covered entity.

#### e. National Identifiers

As covered entities, endorsed sponsors must comply with the standards, implementation specifications, and requirements of 45 CFR parts 160 and 162, relating to the use of national identifiers, as of the compliance date of any final rule issued under part 162.

#### f. Security

As covered entities, endorsed sponsors must comply with the standards, implementation specifications, and requirements of the HIPAA Security Rule ("Security Rule") set forth in 45 CFR parts 160 and 164, subparts A and C to ensure the confidentiality, integrity, and availability of all electronic protected health information they create, receive, maintain or transmit as of the compliance date of the final Security Rule (April 15, 2005). In addition, endorsed sponsors as covered entities must have appropriate administrative, technical and physical safeguards in place to protect the privacy of beneficiary information under 45 CFR 164.530(c) of the Privacy Rule. An applicant must include in its application the following:

- An attestation that as of the date upon which it will begin enrollment activities, appropriate administrative, technical and physical safeguards will be in place to protect the privacy of protected health information in accordance with 45 CFR 164.530(c); and
- An attestation that it will meet the standards, requirements, and implementation specifications as set forth in the Security Rule as of the date

it begins enrolling beneficiaries in its endorsed programs, or, if the endorsed sponsor will be unable to provide this attestation, the applicant's plan for coming into compliance with the specifications as set forth in the Security Rule as of the compliance date for the Security Rule.

Endorsed sponsors are encouraged, but not required, to use Information Security Program references as provided by the National Institute of Standards and Technology (NIST), in documenting their efforts to implement reasonable security measures.

We believe these attestation requirements are critical to beneficiary confidence in the Medicare drug discount card program and their decision to enroll in an endorsed program. Furthermore, as endorsed sponsors are using the Medicare name and acting on our behalf in administering transitional assistance, we believe these requirements are important to promoting the continued confidence of beneficiaries in the Medicare program. We specifically require that applicants attest that they will be in compliance with the Security Rule as of their initiation of enrollment activities, or provide their plan for coming into compliance as of the compliance date. This approach will allow us to evaluate whether their information security measures will comply with the Privacy Rule standard under 45 CFR 164.530(c) and whether they will adequately protect the confidentiality, integrity, and availability of discount card enrollees' electronic protected health information.

#### 10. Document Retention

Section 403.813(b) of our regulations requires endorsed sponsors to retain records that they or their subcontractors create, collect, or maintain while participating in the Medicare drug discount card program for at least six years following termination of the transition period. This retention period may be extended by the Secretary if an endorsed sponsor's records relate to an ongoing investigation, litigation, or negotiation by the Secretary, the OIG, the Department of Justice, or a State, or such documents otherwise relate to suspicions of fraud and abuse or violations of Federal or State law.

We recognize that under the Privacy Rule, CMS, as a covered entity, must require its business associates, upon termination of the contract, to return or destroy protected health information created or received in their capacity as business associates, or if such return or destruction is not feasible, to extend the contract protections to the retained

information and limit further uses and disclosures to the purposes that made the return or destruction infeasible. Our record retention policy will make it infeasible for endorsed sponsors to return or destroy protected health information, as they will be required to retain all program information for at least six years after termination of the program. Therefore, as required by the Privacy Rule, the business associate contract protections for the retained information will continue to be applied and any further use or disclosure of the information will be limited to health care operations and health oversight activities that made return or destruction of the information infeasible, as well as other uses or disclosures that may be required by law.

In addition, our record retention policy will require endorsed sponsors to continue to apply security and privacy protections to the record and the information contained therein to the same extent endorsed sponsors are required to do so prior to termination. We establish this requirement under the authority granted the Secretary under section 1860D-31(h)(8) of the Act to protect and promote the interests of beneficiaries. The interests of beneficiaries are furthered by continuing to protect the confidentiality, integrity, and availability of their protected health information for so long as these records are retained by an endorsed sponsor.

We believe our retention policy is necessary to preserve our ability and that of other Federal and State agencies to exercise appropriate oversight over endorsed sponsors and protect the interests of beneficiaries. We believe six years represents an appropriate time period for this requirement because there is a six year statute of limitations on bringing actions for civil monetary damages under section 1860D-31(i)(3) of the Act against endorsed sponsors that knowingly engage in conduct that violates the requirements of section 1860D-31 or our regulations. Our record retention policy is subject to enforcement under § 403.820(a) of our regulations.

#### 11. Endorsed Sponsor Reporting

Section 1860D-31(h)(4) of the Act provides that endorsed sponsors shall pass on negotiated prices to discount card enrollees, including discounts with pharmacies and manufacturers, to the extent disclosed to the Secretary. Further, section 1860D-31(i)(1) of the Act provides that endorsed sponsors shall disclose to the Secretary (in a manner specified by the Secretary) information relating to program