

Part C plan who are also enrolled in its endorsed program, to the exclusion of other plan members. In contrast, we will consider a Part C organization as acting in its capacity as a Part C plan if it directs its marketing to all or a subset of its Part C plan membership, including those not enrolled in its endorsed program, and, to the extent it uses individual information, such information was not collected or maintained under the Part C organization's endorsed program. Similarly, we will consider an organization's Web site listing its full range of products and services, including but not limited to its endorsed program, as targeted to the public at-large; however, we will consider its web pages specifically describing its endorsed program as targeting potential discount card enrollees, and therefore such web pages may not include information related to products and services offered outside the scope of endorsement.

Section 403.813(a) of our regulations is not enforceable under HIPAA but will be enforced by CMS under the Medicare drug discount card program.

5. Other Uses and Disclosures Without Authorization

Under 1860D–31(i)(1) of the Act and as discussed in section II.A., II.C., and II.F. of this document, endorsed sponsors are required to disclose to the Secretary certain information, some of which may contain protected health information. The Privacy Rule at 45 CFR 164.512(a) permits covered entities to use or disclose protected health information without individual authorization where the use or disclosure is required by other law. Thus, the Privacy Rule permits endorsed sponsors to make the required disclosures to the Secretary without beneficiary authorization. Similarly, the Privacy Rule at 45 CFR 164.512(d) permits covered entities to use or disclose protected health information without individual authorization to a health oversight agency for oversight activities that are authorized by law. Both of these provisions would permit endorsed sponsors to provide CMS with the information needed for the Secretary's oversight and reporting requirements.

6. Uses and Disclosures Requiring an Authorization

For uses and disclosures of protected health information that are not otherwise permitted under the Privacy Rule, an endorsed sponsor must obtain a beneficiary's written authorization for such uses or disclosures in accordance

with 45 CFR 164.508. For example, a Medicare beneficiary may authorize the endorsed sponsor to disclose his/her protected health information to a third party, such as an employer. However, as explained above and provided for in § 403.813(a)(2) of our regulations, an endorsed sponsor may not market products or services outside the scope of its endorsement under the Medicare drug discount card program even if it obtains from discount card enrollees authorization to do so. Additional information about this marketing prohibition can be found above in this section and also in section II.C.5 of this document.

7. Notice of Privacy Practices

In accordance with the Privacy Rule at 45 CFR 164.520, prior to enrolling a beneficiary in its endorsed program, or at the time of enrollment, an endorsed sponsor must notify each beneficiary as to how the endorsed sponsor is permitted or required to use and disclose the beneficiary's protected health information, as well as of the beneficiary's rights and the endorsed sponsor's duties with respect to that information. The notice must be in plain language and clearly explain these rights and the uses and disclosures permitted or required under this rule and other applicable law, including that the endorsed sponsor may use or disclose protected health information to communicate about products and services offered by an endorsed sponsor inside, and only inside, the scope of its endorsement. The notice may be combined with other information and outreach materials, provided that the content requirements of the Privacy Rule are fully met.

8. Endorsed Sponsors as Business Associates

As defined in the Privacy Rule, a business associate is a person or entity that performs or assists in the performance of certain functions or activities on behalf of, or provides certain services to, a covered entity, that involve the use or disclosure of individually identifiable health information. The Privacy Rule requires that the covered entity obtain satisfactory assurances, usually in the form of a written contract, from the business associate that the business associate will appropriately safeguard the protected health information it creates or receives on behalf of the covered entity. The contract or other written arrangement between the covered entity and its business associate must meet the requirements at 45 CFR 164.504(e).

For purposes of administering transitional assistance, endorsed sponsors are business associates of CMS under the Privacy Rule. Transitional assistance will be a benefit offered and paid for by the Medicare program, a health plan, with CMS contracting with endorsed sponsors to administer transitional assistance on behalf of CMS in conjunction with their other responsibilities under the Medicare drug discount card program. As such, the contract between CMS and endorsed sponsors will include the terms necessary to satisfy the requirements of the Privacy Rule at 45 CFR 164.504(e).

The application of the Privacy Rule to endorsed sponsors under our regulations does not affect business associate arrangements or requirements between the endorsed sponsor and one or more covered entities for activities that are outside of the endorsed drug card program. However, because an endorsed sponsor is also a covered entity, when an endorsed sponsor is acting as a business associate of another covered entity, the endorsed sponsor will violate the Privacy Rule if it violates its business associate contract with the other covered entity (*see* 45 CFR 164.502(e)(1)(iii)).

9. Enforcement by the HHS Office for Civil Rights

The HHS Office for Civil Rights (OCR) is responsible for implementing and enforcing the HIPAA Privacy Rule. OCR has authority to investigate complaints and to conduct compliance reviews, and may impose civil money penalties on covered entities for violations where appropriate. Thus, any violations by an endorsed sponsor with respect to its obligations under the Privacy Rule as a covered entity are subject to such enforcement by OCR. OCR maintains a Web site with Frequently Asked Questions and other compliance guidance at <http://hhs.gov/ocr/hipaa>.

OCR's enforcement authority pertains only to the HIPAA Privacy Rule. Thus, any violations with respect to compliance with the other HIPAA Administrative Simplification Rules or proper operation of an endorsed program will be enforced by CMS. In addition, if an endorsed sponsor's actions also violate the requirements of the Medicare drug discount card program, such actions also may be sanctioned under § 403.820(a) of our regulations. See section II.F. of this document for further information about CMS oversight and monitoring of endorsed sponsors.