DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (214) 767-4056, (800) 368-1019
FAX - (214) 767-0432
TDD - (214) 767-8640
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region VI
1301 Young Street, Suite 1169
Dallas, TX 75202

OCT 10 2012

(b)(6),(b)(7)(C)

Re: (b)(6),(b)(7)(C) **v. CVS Caremark**
OCR Transaction Number: 12-148178

Dear (b)(6),(b)(7)(C)

On August 28, 2012, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), Region VI, received your complaint alleging that CVS Caremark (CVS), the covered entity, has violated the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, Subparts A and E, the Privacy Rule).

Specifically you allege that on or near August 20, 2012, CVS sent you an invoice containing prescription information for your ex-husband, (b)(6),(b)(7)(C) You further allege that you contacted CVS via phone and spoke with a customer service representative who disclosed details about (b)(6),(b)(7)(C) health insurance information. These allegations could reflect a violation of 45 C.F.R. §§ 164.502(a) 164.510(b), and 164.530(c). Thank you for bringing this matter to OCR's attention. Your complaint plays an integral part in OCR's enforcement efforts.

OCR enforces the Privacy, Security, and Breach Notification Rules, and also enforces Federal civil rights laws which prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and under certain circumstances, sex and religion.

A covered entity may not use or disclose protected health information except as permitted or required by the Privacy Rule. As long as an individual does not object, a covered entity is allowed to share or discuss with the individual's family, friends, or other persons identified by the individual the protected health information that is directly relevant to such person's involvement with the individual's care or payment for care.

The covered entity may ask the individual's permission, may tell the individual that the covered entity plans to discuss the information and give the individual an opportunity to object, or may decide, using the covered entity's professional judgment, that the individual does not object. However, in any of these cases, the covered entity may discuss **only** the information that the person involved needs to know about the individual's care or payment for their care.

The minimum necessary provision of the Privacy Rule also requires the covered entity to limit access to protected health information by identifying: the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access.

Finally, a covered entity must provide a process for individuals to make complaints concerning

the covered entity's policies and procedures required by the Privacy Rule or its compliance with such policies and procedures or with the requirements of the Privacy Rule. 45 C.F.R. § 164.530(d)(1).

We have carefully reviewed your complaint against CVS and have determined to resolve this matter informally through the provision of technical assistance to CVS. Should OCR receive a similar allegation of noncompliance against CVS in the future, OCR may initiate a formal investigation of that matter.

Based on the foregoing, OCR is closing this case without further action, effective the date of this letter. OCR's determination as stated in this letter applies only to the allegations in this complaint that were reviewed by OCR.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions regarding this matter, please contact Betty Robinson, Investigator, at (214) 767-4073.

Sincerely,

Ralph D. Rouse
Regional Manager, Region VI

DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF THE SECRETARY

Voice - (214) 767-4056, (800) 368-1019
FAX - (214) 767-0432
TDD - (214) 767-8940
http://www.hhs.gov/ocr/

Office for Civil Rights, Region VI
1301 Young Street, Suite 1169
Dallas, TX 75202

OCT 10 2012

(b)(6),(b)(7)(C)
CVS Caremark
CVS/Pharmacy Privacy Officer
9501 E. Shea Blvd.
Scottsdale, AZ 85260

Re: (b)(6),(b)(7)(C) **v. CVS Caremark**
OCR Transaction Number: 12-148178

Dear (b)(6),(b)(7)(C):

On August 28, 2012, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), Region VI, received a complaint alleging that CVS Caremark (CVS), the covered entity, has violated the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, Subparts A and E, the Privacy Rule).

Specifically, the complainant, (b)(6),(b)(7)(C) alleges that on or near August 20, 2012, CVS sent her an invoice containing prescription information for her ex-husband, (b)(6),(b)(7)(C) The complainant further alleges that she contacted CVS via phone and spoke with a customer service representative who disclosed details about (b)(6),(b)(7)(C) health insurance information. These allegations could reflect a violation of 45 C.F.R. §§ 164.502(a) 164.510(b), and 164.530(c)

OCR enforces the Privacy, Security, and Breach Notification Rules, and also enforces Federal civil rights laws which prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and under certain circumstances, sex and religion.

Pursuant to the Privacy Rule, a covered entity may not use or disclose protected health information (PHI) except as permitted or required by the Privacy Rule. As long as an individual does not object, a covered entity is allowed to share or discuss the individual's health information with the individual's family, friends, or others involved in the individual's care or payment for their cared.

The covered entity may ask the individual's permission, may tell the individual that the covered entity plans to discuss the information and give the individual an opportunity to object, or may decide, using the covered entity's professional judgment, that the individual does not object. However, in any of these cases, the covered entity may discuss **only** the information that the person involved needs to know about the individual's care or payment for their care.

The minimum necessary provision of the Privacy Rule also requires the covered entity to limit access to protected health information by identifying: the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access.

Finally, a covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by the Privacy Rule or its compliance with such policies and procedures or with the requirements of the Privacy Rule. 45 C.F.R. § 164.530(d)(1).

In this matter, the complainant alleges that the complainant's ex-husband's PHI was impermissibly disclosed to the complainant or that the complainant's ex-husband's PHI was otherwise impermissibly used by an employee of CVS. Pursuant to its authority under 45 C.F.R. §§ 160.304(a) and (b), OCR has determined to resolve this matter informally through the provision of technical assistance to CVS. To that end, OCR has enclosed material explaining the Privacy Rule provisions related to Disclosures to Family and Friends, the Minimum Necessary Requirement, and Reasonable Safeguards.

It is our expectation that you will review these materials closely and share them with your staff as part of the Health Insurance Portability and Accountability Act (HIPAA) training you provide to your workforce. It is also our expectation that you will access and determine whether there may have been an incident of noncompliance as alleged by the complainant in this matter, and if so, to take the steps necessary to ensure such noncompliance does not occur in the future. Please contact OCR if you need further information regarding the allegations in this matter. Should OCR receive a similar allegation of noncompliance against CVS in the future, OCR may initiate a formal investigation of that matter.

Based on the foregoing, OCR is closing this case without further action, effective the date of this letter. OCR's determination as stated in this letter applies only to the allegations in this complaint that were reviewed by OCR.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions regarding this matter, please contact Betty Robinson, Investigator, at (214) 767-4073.

Sincerely,

Ralph D. Rouse
Regional Manager, Region VI

Enclosures: Disclosures to Family and Friends
The Minimum Necessary Requirement
Reasonable Safeguards

DISCLOSURES TO FRIENDS AND FAMILY
45 C.F.R. § 164.510(b)

The Privacy Rule does not require a health care provider or health plan to share information with a patient's family or friends, unless they are the patient's personal representatives. The law does permit providers and plans to share information with a patient's family or friends in certain circumstance. A health care provider or health plan may share relevant information with family members or friends involved in the patient's health care or payment for the patient's health care, if the patient tells the provider or plan that it can do so, or if the patient does not object to sharing of the information. For example, if the patient does not object, the patient's doctor could talk with the friend who goes with the patient to the hospital or a family member who pays the patient's medical bill.

A provider or plan may also share relevant information with these persons if, using its professional judgment, it believes that the patient does not object. For example, if a patient sends a friend to pick up your prescription for the patient, the pharmacist can assume that the patient does not object to their being given the medication. When the patient is not there or is injured and cannot give their permission, a provider may share information with these persons when it decides that doing so would be in the patient's best interest.

Frequently Asked Questions

Q: Does the HIPAA Privacy Rule permit a doctor to discuss a patient's health status, treatment, or payment arrangements with the patient's family and friends?

A: Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on their professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient's mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient's payment options with her adult daughter.
- A doctor may instruct a patient's roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient's treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient's incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising

professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). Thus, for example:

- A surgeon may, if consistent with such professional judgment, inform a patient's spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient's progress and prognosis.
- A doctor may, if consistent with such professional judgment, discuss an incapacitated patient's condition with a family member over the phone.

In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient's best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.

Q: If the patient is not present or is incapacitated, may a health care provider still share the patient's health information with family, friends, or others involved in the patient's care or payment for care?

A: Yes. If the patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient. When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care. The health care provider may discuss only the information that the person involved needs to know about the patient's care or payment. Here are some examples:

- A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.
- A pharmacist may give a prescription to a patient's friend who the patient has sent to pick up the prescription.
- A hospital may discuss a patient's bill with her adult son who calls the hospital with questions about charges to his mother's account.
- A health care provider may give information regarding a patient's drug dosage to the patient's health aide who calls the provider with questions about the particular prescription.

BUT:

- A nurse may <u>not</u> tell a patient's friend about a past medical problem that is unrelated to the patient's current condition.
- A health care provider is <u>not</u> required by HIPAA to share a patient's information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

HIPAA Privacy Rule Disclosures to a Patient's Family, Friends, or Others Involved in the Patient's Care or Payment for Care

	Family Member or Friend	Other Persons
Patient is present and has the capacity to make health care decisions	Provider may disclose relevant information if the provider does one of the following: (1) Obtain the patient's agreement; (2) Gives the patient an opportunity to object and the patient does not object; (3) Decides from the circumstances, based on professional judgment, that the patient does not object Disclosure may be made in person, over the phone, or in writing	Provider may disclose relevant information if the provider does one of the following: (1) Obtain the patient's agreement; (2) Gives the patient an opportunity to object and the patient does not object; (3) Decides from the circumstances, based on professional judgment, that the patient does not object Disclosure may be made in person, over the phone, or in writing
Patient is not present or is incapacitated	Provider may disclose relevant information if, based on professional judgment, the disclosure is in the patient's best interest. Disclosure may be made in person, over the phone, or in writing. Provider may use professional judgment and experience to decide if it is in the patient's best interest to allow someone to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of health information for the patient.	Provider may disclose relevant information if the provider is reasonably sure that the patient has involved the person in the patient's care and in his or her professional judgment, the provider believes the disclosure to be in the patient's best interest. Disclosure may be made in person, over the phone, or in writing. Provider may use professional judgment and experience to decide if it is in the patient's best interest to allow someone to pick up filled prescriptions, medical supplies, X-rays, or other

		similar forms of health information for the patient.

THE MINIMUM NECESSARY REQUIREMENT
45 C.F.R. §§ 164.502(b) and 164.514(d)

Background

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

How the Rule Works

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

Uses and Disclosures of, and Requests for, Protected Health Information

For uses of protected health information, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not

required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification. For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit the protected health information disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required. For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of protected health information necessary to accomplish the purpose of a non-routine disclosure or request. Non-routine disclosures and requests must be reviewed on an individual basis in accordance with these criteria and limited accordingly. Of course, where protected health information is disclosed to, or requested by, health care providers for treatment purposes, the minimum necessary standard does not apply.

Reasonable Reliance

In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).
- Another covered entity.
- A professional who is a workforce member or business associate of the covered entity holding the information and who states that the information requested is the minimum necessary for the stated purpose.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The Rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

Frequently Asked Questions

Q: How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

A: The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the

unnecessary sharing of medical information.

The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.

Q: Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time the entire medical record is disclosed?

A: No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a covered entity may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes. The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who is the subject of the protected health information.

Q: In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigning office space and upgrading computer systems, in order to comply with the HIPAA Privacy Rule's minimum necessary requirements?

A: No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to protected health information to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small,

solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. In this case, appropriate training of employees may be sufficient. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the Privacy Rule.

Reasonable Safeguards

45 C.F.R. § 164.530 (c)

A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 C.F.R. §164.530 (c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals' health information – for instance:

- By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- By isolating or locking file cabinets or records rooms; or
- By providing additional security, such as passwords, on computers maintaining personal information.

Protection of patient confidentiality is an important practice for many health care and health information management professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.