



Capital One Financial Corporation Employee Welfare Plan

HIPAA Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Introduction

You are receiving this Notice of Privacy Practices (Notice) as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) because you are a participant or may become a participant in a group health plan component of the Capital One Financial Corporation Welfare Plan (the Plan) sponsored by Capital One Financial Corporation (Capital One). The group health plan components of the Plan include health, dental, vision, and health flexible spending accounts. This Notice applies to those benefits but does not apply to non-health plan components under the Plan such as disability and life insurance benefits.

Effective Date

This Notice was originally effective April 14, 2003 and has been modified as required by law or as otherwise appropriate. This version is effective November 10, 2021. It reflects applicable changes since the previous version published on June 3, 2019.

Protected Health Information (PHI)

The HIPAA privacy rules regulate the use and disclosure by the Plan of “protected health information” (PHI). PHI includes all individually identifiable health information transmitted or maintained by the Plan, regardless of form (oral, written, electronic). Individually identifiable health information is health information that identifies you or creates a reasonable basis to believe that it could be used to identify you, including information relating to your health condition or receipt of health care. Health information that is merely in summary form and that does not identify you as its subject is not PHI and may be used or disclosed by the Plan without restriction under HIPAA.

The vast majority of health information the Plan receives is not PHI. In most cases, the Plan only receives summary health information without identifying information. This type of information is typically provided by the Plan’s healthcare provider and other vendors (Business Associates) and is not PHI. The majority of PHI received by the Plan is limited to information shared directly by associates for purposes of asking benefit-related questions, making claims inquiries and similar escalations. It is that information

that is the subject of this Notice. Unlike the Plan, Capital One's Business Associates receive substantial PHI and are required to comply with the HIPAA rules applicable to them. This Notice is focused on use and disclosures of PHI received by the Plan, rather than by its Business Associates. Nevertheless, some sections below address PHI received by Business Associates to ensure you understand the rules regarding appropriate use of PHI, particularly, when authorization is required and when it is not.

Because the Plan receives some limited PHI, it is required by HIPAA to take reasonable steps to ensure the privacy of your PHI and to inform you about:

- The Plan's uses and disclosures of PHI;
- Your privacy rights with respect to your PHI;
- The Plan's duties with respect to your PHI;
- Your right to file a complaint with the Plan and to the Secretary of the U.S. Department of Health and Human Services; and
- The person or office to contact for further information about the Plan's privacy practices.

HIPAA rules permit the Plan to use or disclose your PHI for certain purposes without your permission. The following categories describe the different ways the Plan (and in some cases its Business Associates) may use and disclose your PHI with or without your permission. For each category of uses or disclosures we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

Section 1. Uses and Disclosures of PHI

Required PHI Uses and Disclosures

Disclosures to you

Upon your request, the Plan is required to give you access to PHI maintained by the Plan in order to inspect and copy it.

Disclosures to the Department of Health and Human Services

Use and disclosure of your PHI may be required by the Secretary of the Department of Health and Human Services to investigate or determine the Plan's compliance with the privacy regulations.

Uses and Disclosures Not Requiring Your Permission

Uses and disclosures to carry out treatment, payment and health care operations.

The Plan and its Business Associates are permitted by law to use PHI to carry out certain functions under HIPAA, including treatment, payment and health care operations,

without your consent, authorization or opportunity to agree or object. The Plan and its Business Associates are also permitted to disclose PHI to Capital One for purposes related to treatment, payment and health care operations. Capital One has amended its plan documents to protect your PHI as required by federal law.

Treatment. The Plan or its Business Associates may use or disclose your PHI to facilitate medical treatment or service by health care providers.

For example, Capital One's Business Associates may disclose to a treating orthodontist the name of your treating dentist so that the orthodontist may ask for your dental X-rays from the treating dentist.

Payment. The Plan or its Business Associates may use or disclose your PHI to determine your eligibility for Plan benefits, to facilitate payment for treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. Such uses (typically performed by our Business Associates) may include, but are not limited to billing, claims management, subrogation, plan reimbursement, reviews for medical necessity and appropriateness of care and utilization review and pre-authorizations.

For example, Capital One's Business Associates may tell a doctor whether you are eligible for coverage or what percentage of the bill will be paid by the Plan.

Health care operations. The Plan or its Business Associates may use or disclose your PHI for other activities related to the administration of the Plan, including but not limited to quality assessment and improvement, and reviewing competence or qualifications of health care professionals. Capital One's Business Associates may also use or disclose your PHI for purposes of underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts. Such activities may also include disease management, case management, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse compliance programs, business planning and development, business management and general administrative activities.

For example, Capital One's Business Associates may use information about your claims to refer you to a disease management program, project future benefit costs or audit the accuracy of its claims processing functions. Or, the Plan may use or disclose your PHI for purposes of annual renewals with benefits carriers and annual rate setting.

Uses and disclosures to Business Associates.

As noted above, the Plan contracts with Business Associates to perform various functions on the Plan's behalf or to provide certain types of services. In order to perform these functions or to provide these services, Business Associates will receive, create, maintain, use and/or disclose your PHI, but only after they agree in writing with us to implement appropriate safeguards regarding your PHI.

For example, the Plan may disclose your PHI to a Business Associate to help facilitate resolution of a question or administration of a claim which you raise with the Plan, but only if the Business Associate has entered into a Business Associate contract with us.

Uses and disclosures to certain Capital One associates for plan administration functions.

The Plan may disclose your PHI to certain designated associates who are involved in the administration of the Plan. These disclosures will be made in connection with Capital One's role as the sponsor of the Plan, and will be made to enable the appropriate associates to carry out their duties in administering the Plan. Capital One has instituted policies and procedures to help ensure that your PHI is made available only to those individuals who need it to perform important Plan functions. Such associates will only use or disclose information as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your PHI will not be used for employment actions or decisions or without your specific authorization.

Other uses and disclosures not requiring your permission.

In addition, federal law allows the Plan to use or disclose your PHI without your consent, authorization or opportunity to object in under the following circumstances:

- 1 Required or authorized by law. The Plan may disclose your PHI when required by federal, state or local law, or when authorized for intelligence, counterintelligence and other national securities activities.
- 2 Public health risks. The Plan may disclose your PHI when public health risks exist. These actions generally include the following:
 - o to prevent or control disease, injury, or disability;
 - o to report births and deaths;
 - o to report child abuse or neglect;
 - o to report reactions to medications or problems with products;
 - o to notify people of recalls of products they may be using;
 - o to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.
- 3 Health oversight activities. The Plan may disclose your PHI to a public health oversight agency for oversight activities authorized by law. This includes uses or disclosures in civil, administrative or criminal investigations; inspections; licensure or disciplinary actions (for example, to investigate complaints against providers); and other activities necessary for appropriate oversight of government benefit programs (for example, to investigate Medicare or Medicaid fraud).
- 4 Lawsuits or disputes. The Plan may disclose your PHI when required for judicial or administrative proceedings. For example, your PHI may be disclosed in response to a subpoena or discovery request provided certain conditions are met. One of those conditions is that satisfactory assurances must be given to the Plan that the requesting party has made a good faith attempt to provide written notice to you, and the notice provided sufficient information about the proceeding to permit you to raise an objection and no objections were raised or were resolved in favor of disclosure by the court or tribunal.

- 5 Law enforcement purposes. The Plan may disclose your PHI when required for law enforcement purposes such as:
 - in response to a court order, subpoena, warrant, summons or similar process;
 - to identify or locate a suspect, fugitive, material witness, or missing person.
 - to provide information about the victim of a crime if, under certain limited circumstances, we are unable to obtain the victim's agreement;
 - to provide information about a death that we believe may be the result of criminal conduct; and
 - to provide information about criminal conduct.
- 6 Coroners, medical examiners and funeral directors, The Plan may disclose your PHI when required to be given to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as authorized by law. The Plan may also disclose your PHI to funeral directors, as necessary to carry out their duties with respect to the decedent.
- 7 Organ and tissue donation. The Plan may disclose your PHI to organizations that handle organ procurement or organ, eye, or tissue transplantation to an organ donation bank, as necessary to facilitate organ or tissue donation and transplant.
- 8 Research. The Plan may disclose PHI for research when the individual identifiers have been removed, or when an institutional review board or privacy board has reviewed the research proposal and established protocols to ensure the privacy of the requested information, and approves the research.
- 9 Public safety. The Plan may disclose your PHI when consistent with applicable law and standards of ethical conduct, the Plan, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the disclosure is to a person reasonably able to prevent or lessen the threat, including the target of the threat.
- 10 Workers compensation. The Plan may disclose your PHI when authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law.

Except as otherwise indicated in this notice, uses and disclosures will be made only with your written authorization subject to your right to revoke such authorization.

Uses and Disclosures Requiring an Opportunity to Agree or Disagree

Disclosure of your PHI to family members, other relatives and your close personal friends is allowed if the information is directly relevant to the family or friend's involvement with your care or payment for that care; and

- You are incapacitated and/or there is an emergency situation; or
- You have either agreed to the disclosure or have been given an opportunity to object and have not objected.

Uses and Disclosures Requiring Written Authorization

Other uses or disclosures of your PHI not described above will only be made with your written authorization. You may revoke written authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation

Section 2. Rights of Individuals

Right to Request Restrictions on PHI Uses and Disclosures

You may request the Plan to restrict uses and disclosures of your PHI to carry out treatment, payment or health care operations, or to restrict uses and disclosures to family members, relatives, friends or other persons identified by you who are involved in your care or payment for your care. The Plan is not required to agree to your request. However, the Plan must agree to restrictions as to the disclosure of PHI for payment or health care operations if the information pertains only to a service that you have paid for out of pocket in full, unless the disclosure is otherwise required by law or for treatment purposes.

The Plan will accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations.

You or your personal representative will be required to complete a form to request restrictions on uses and disclosures of your PHI.

Such requests may be made to the applicable Claims Administrator or to the Plan's Privacy Committee. See Section 5 for contact information.

Right to Inspect and Copy PHI

You have a right to inspect and obtain a copy of your PHI contained in a "designated record set," for as long as the Plan maintains the PHI.

"Designated Record Set" is defined to include the enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for the group health plan components of the Plan; or other information used in whole or in part by or for the Plan to make decisions about individuals. Since the Plan receives very limited PHI (typically disclosed by associates for purposes of answering questions or facilitating claims), only the limited PHI received by the Plan will be included in an associate's designated record set from the Plan. All other relevant information is maintained by Capital One's Business Associates.

The requested information will be provided by the Plan within 30 days if the information is maintained on site or within 60 days if the information is maintained offsite. A single 30-day extension is allowed if the Plan is unable to comply with the deadline.

Requests for access to PHI should be made to the Plan's Privacy Committee. See Section 5 for contact information.

If access is denied, you or your personal representative will be provided with a written denial setting forth the basis for the denial, a description of how you may exercise those review rights and a description of how you may complain to the Secretary of the U.S. Department of Health and Human Services.

Right to Amend PHI

You have the right to request the Plan to amend your PHI or a record about you in a designated record set for as long as the PHI is maintained in the designated record set. The Plan may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, it may deny your request if you ask to amend information that:

- is not part of the medical information kept by or for the Plan;
- was not created by the Plan, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information that you would be permitted to inspect and copy; or
- is already accurate and complete.

If we deny your request, you have the right to file a statement of disagreement with the Plan and any future disclosures of the disputed information will include your statement.

The Plan has 60 days after the request is made to act on the request. A 30-day extension is allowed if the Plan is unable to comply with the deadline. If the request is denied in whole or part, the Plan must provide you with a written denial that explains the basis for the denial. You or your personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosures of your PHI.

Requests for amendment of PHI in a designated record set should be in writing, should provide a reason to support your requested amendment and should be made to the Plan's Privacy Committee. See Section 5 for contact information.

Right to Receive an Accounting of PHI Disclosures

At your request, the Plan will also provide you with an accounting of disclosures by the Plan of your PHI during the six years prior to the date of your request. Such accounting generally need not include PHI disclosures made: (1) to carry out treatment, payment or health care operations; (2) to individuals about their own PHI; or (3) prior to the compliance date. However, you may receive information on disclosures of your health information going back for three years for treatment, payment and health care operations disclosures, if the Plan maintains electronic health records of such data.

If the accounting cannot be provided within 60 days, an additional 30 days is allowed if the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided.

If you request more than one accounting within a 12-month period, the Plan will charge a reasonable, cost-based fee for each subsequent accounting.

Such requests can be made to the Plan's Privacy Committee. See Section 5 for contact information.

Right to be Notified of a Breach

You have the right to be notified in the event the Plan discovers a breach of unsecured PHI. A reportable breach occurs when the unauthorized acquisition, access, use, or disclosure of unsecured PHI compromises the security or privacy of the protected health information (i.e. poses a significant risk of financial, reputational, or other harm to the individual).

Right to Receive a Paper Copy of This Notice Upon Request

You have a right to receive a paper copy of this Notice even if you have already received a copy electronically. To obtain a paper copy of this Notice, contact the HR Help Center at 1-888-376-8836. You may also obtain a copy of this notice on Pulse by searching for "HIPAA."

A Note about Personal Representatives

You may exercise your rights through a personal representative by completing a Designated Recipient form. Your personal representative will be required to produce evidence of his/her authority to act on your behalf before that person will be given access to your PHI or allowed to take any action for you. Proof of such authority may take one of the following forms:

- A power of attorney for health care purposes, notarized by a notary public;
- A court order of appointment of the person as the conservator or guardian of the individual; or
- An individual who is the parent of a minor child.

The Plan retains discretion to deny access to your PHI to a personal representative to provide protection to those vulnerable people who depend on others to exercise their rights under these rules and who may be subject to abuse or neglect. This also applies to personal representatives of minors.

Section 3. The Plan's Duties

The Plan is required by law to maintain the privacy of PHI and to provide individuals (participants and beneficiaries) with notice of their legal duties and privacy practices.

The Plan reserves the right to change its privacy practices and to apply the changes to any PHI received or maintained by the Plan prior to that date. If a privacy practice is changed, a revised version of this notice will be provided to all past and present participants and beneficiaries for whom the Plan still maintains PHI. You will receive a copy of any revised notice from the Plan by mail or by email if you agree to delivery by email.

Any revised version of this notice will be distributed within 60 days of the effective date of any material change to the uses or disclosures, the individual's rights, the duties of the Plan or other privacy practices stated in this notice.

Minimum Necessary Standard

When using or disclosing PHI or when requesting PHI from another covered entity, the Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations.

However, the minimum necessary standard will not apply to the following situations:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual;
- Disclosures made to the Secretary of the U.S. Department of Health and Human Services;
- Uses or disclosures that are required by law; and
- Uses or disclosures that are required for the Plan's compliance with legal regulations.

This notice does not apply to information that has been de-identified. De-identified information is information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

In addition, the Plan may use or disclose "summary health information" to Capital One for obtaining premium bids or modifying, amending or terminating the Plan, which summarizes the claims history, claims expenses or type of claims experienced by individuals for whom Capital One has provided health benefits under the Plan; and from which identifying information has been deleted in accordance with HIPAA.

Section 4. Your Right to File a Complaint With the Plan or the HHS Secretary

If you believe that your privacy rights have been violated or if you have a complaint about the Plan's notification process for breaches of unsecured PHI, you may complain to the Plan's Privacy Committee. See Section 5 for contact information. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, 200 Independence Avenue S.W., Washington, D.C. 20201

or calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/. You will not be penalized, or in any way retaliated against for filing a complaint with the Office for Civil Rights or with the Plan.

Section 5. Whom to Contact at the Plan for More Information

If you have any questions regarding this notice or the subjects addressed in it or wish to enforce your rights under this notice you may contact the Plan's Privacy Committee:

Capital One Financial

Attn: Privacy Committee

C/O Pamela Ventura

15000 Capital One Drive

Richmond, VA 23238

(804) 690-1348

pamela.Ventura@capitalone.com

To obtain a copy of this notice, please visit Pulse or contact the HR Help Center at 1-888-376-8836 to request a paper copy.

Conclusion

PHI use and disclosure by the Plan is regulated by a federal law known as HIPAA (the Health Insurance Portability and Accountability Act). You may find these rules at 45 *Code of Federal Regulations* Parts 160 and 164. This notice merely summarizes the regulations. The regulations will supersede any discrepancy between the information in this notice and the regulations.