JENNER & BLOCK LLP
Vincent E. Lazar (admitted *pro hac vice*)
Derek L. Wright (admitted *pro hac vice*)
Angela M. Allen (admitted *pro hac vice*)
353 N. Clark Street
Chicago, IL 60654
Telephone: (312) 222-9350
Facsimile: (312) 527-0484
Email: vlazar@jenner.com
dwright@jenner.com
aallen@jenner.com

HAYNES AND BOONE, LLP
Charles A. Beckham, Jr. (TX #02016600)
Ian T. Peck (TX #24013306)
Martha Wyrick (TX #24101606)
2801 N. Harwood Street, Ste. 2300
Dallas, TX 75201
Telephone: (214) 651-5000
Facsimile: (214) 651-5940
Email: charles.beckham@haynesboone.com
ian.peck@haynesboone.com
martha.wyrick@haynesboone.com

Counsel for the Debtors and Debtors in Possession

IN THE UNITED STATES BANKRUPTCY COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

In re:	)	Chapter 11
OMNICARE, LLC, *et al.*,[1]	)	Case No. 25-80486 (SGJ)
Debtors.	)	(Jointly Administered)

NOTICE OF FILING OF DECLARATION OF MARCY WILDER, PRIVACY EXPERT, IN SUPPORT OF DEBTORS' SALE MOTION

PLEASE TAKE NOTICE that on November 7, 2025, the Debtors filed their *Motion for Entry of an Order (I)(A) Approving Bidding Procedures and the Form and Manner of Notice Thereof, (B) Authorizing the Selection of Stalking Horse Bidder(s) and Approving Bid Protections, (C) Establishing Bid Deadlines and Scheduling the Auction and Sale Hearing(s), and*

[1] The last four digits of Omnicare, LLC's federal tax identification number are 1351. There are 110 Debtors in these chapter 11 cases, which are being jointly administered for procedural purposes only. A complete list of the Debtors and the last four digits of their federal tax identification numbers may be obtained on the website of the Debtors' claims and noticing agent at https://cases.stretto.com/Omnicare. The location of Omnicare, LLC's corporate headquarters and the Debtors' service address is One CVS Drive, Mail Code 1160, Woonsocket, RI 02895.

(D) Establishing Certain Assumption and Assignment Procedures and Approving the Manner of Notice Thereof; and (II) Granting Related Relief [Docket No. 288].

PLEASE TAKE FURTHER NOTICE that on December 3, 2025 and April 14, 2026, the Court entered orders [Docket Nos. 398 and 757] which, among other things, approved bidding procedures (the "**Bid Procedures**")[2] to be used in connection with one or more sales of all or substantially all of the Debtors' assets (the "**Sales**").

PLEASE TAKE FURTHER NOTICE that a hearing to consider approval of a Sale to GenieRX Holdings LLC is scheduled to begin on May 13, 2026 at 1:30 p.m. (prevailing Central Time).

PLEASE TAKE FURTHER NOTICE that on April 3, 2026, the Court entered its *Order (I) Authorizing the Retention and Employment of Marcy Wilder and Hogan Lovells LLP to Provide Expert Services Effective as of December 1, 2025 and (II) Granting Related Relief* [Docket No. 729].

PLEASE TAKE FURTHER NOTICE that the Debtors hereby file the *Declaration of Marcy Wilder, Privacy Expert, in Support of the Debtors' Proposed Sale and Transfer of Personally Identifiable Information and PHI*, attached hereto as **Exhibit 1**.

PLEASE TAKE FURTHER NOTICE that copies of the foregoing pleadings may be obtained (i) at the website established by the Debtors' proposed noticing agent, Stretto, Inc. at https://cases.stretto.com/Omnicare, (ii) from the Court's website at http://www.txnb.uscourts.gov via ECF/Pacer, or (iii) upon request to the undersigned.

[2] Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Bid Procedures or the orders approving the Bid Procedures, as applicable.

Dated: May 4, 2026

Respectfully submitted,

HAYNES AND BOONE, LLP

/s/ Ian T. Peck
Charles A. Beckham, Jr. (TX #02016600)
Ian T. Peck (TX #24013306)
Martha Wyrick (TX #24101606)
2801 N. Harwood Street, Ste. 2300
Dallas, Texas 75201
Telephone: (214) 651-5000
Facsimile: (214) 651-5940
Email: charles.beckham@haynesboone.com
ian.peck@haynesboone.com
martha.wyrick@haynesboone.com

JENNER & BLOCK LLP

Vincent E. Lazar (admitted *pro hac vice*)
Derek L. Wright (admitted *pro hac vice*)
Angela M. Allen (admitted *pro hac vice*)
353 N. Clark Street
Chicago, Illinois 60654
Telephone: (312) 222-9350
Facsimile: (312) 527-0484
Email: vlazar@jenner.com
dwright@jenner.com
aallen@jenner.com

Counsel to the Debtors and Debtors in Possession

Exhibit 1

Wilder Declaration

IN THE UNITED STATES BANKRUPTCY COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

In re:	)	Chapter 11
OMNICARE, LLC, *et al.*,[1]	)	Case No. 25-80486 (SGJ)
Debtors.	)	(Jointly Administered)

DECLARATION OF MARCY WILDER, PRIVACY EXPERT, IN SUPPORT OF THE DEBTORS' PROPOSED SALE AND TRANSFER OF PERSONALLY IDENTIFIABLE INFORMATION AND PHI

I, Marcy Wilder, hereby declare under penalty of perjury:

1. I am a licensed attorney and founding partner of the Data, Privacy and Cybersecurity Practice at the law firm Hogan Lovells US LLP. For more than three decades, my practice has focused on health data privacy, cybersecurity, digital health, and related regulatory matters, including advising clients on complex health privacy compliance issues, regulatory investigations, and data governance considerations.

2. Before entering private practice, I served as Deputy General Counsel at the U.S. Department of Health and Human Services ("**HHS**"), where I led the legal team responsible for drafting the privacy and security regulations implementing the Health Insurance Portability and Accountability Act ("**HIPAA**"). Since then, I have advised clients across a range of industries on federal and state privacy requirements, including matters involving the HHS Office for Civil Rights, the Federal Trade Commission, and state attorneys general, as well as broader regulatory

[1] The last four digits of Omnicare, LLC's federal tax identification number are 1351. There are currently 110 debtors (collectively, the "**Company**" or the "**Debtors**") in these chapter 11 cases, which are being jointly administered for procedural purposes only (the "**Chapter 11 Cases**"). A complete list of the debtors and the last four digits of their federal tax identification numbers may be obtained on the website of the debtors' claims and noticing agent at https://cases.stretto.com/Omnicare. The location of Omnicare, LLC's corporate headquarters and the Company's service address is One CVS Drive, Mail Code 1160, Woonsocket, RI 02895.

issues for leading health and technology companies. I am routinely called upon to advise on proposed regulatory and legislative changes that impact the electronic health environment.

3. I received my Juris Doctor from Stanford Law School and Bachelor of Arts degree from Union College. I am admitted to practice law in the District of Columbia, California, and before the Supreme Court of the United States.

4. In addition to my legal practice, I am active in professional and industry organizations and have frequently spoken and written on issues related to privacy, cybersecurity and digital health. I have served on the board of directors of the eHealth Initiative and am a member of organizations including the American Health Lawyers Association. My work in health privacy and data security has been recognized by professional rankings and publications, including *Chambers USA* and inclusion in the *Legal 500* Hall of Fame.

5. In connection with the Chapter 11 Cases filed by the Company pursuant to chapter 11 of title 11 of the United States Code (the "**Bankruptcy Code**") on September 22, 2025 (the "**Petition Date**"), I conducted a review of the Company's privacy policies and certain practices.[2] I submit this declaration (a) in support of the Company's transfer of Personally Identifiable Information and PHI (each defined below) as part of the proposed sale to GenieRx Holdings LLC, the approval of which is currently set for hearing on May 13, 2026 (the "**Sale**") and (b) to demonstrate that the Company's transfer of Personally Identifiable Information and PHI does not necessitate the appointment of a consumer privacy ombudsperson pursuant to section 363(b)(1) of the Bankruptcy Code.

[2] The Company was authorized to retain me to provide expert services and prepare this Declaration pursuant to the *Order (I) Authorizing the Retention and Employment of Marcy Wilder and Hogan Lovells LLP to Provide Expert Services Effective as of December 1, 2025 and (II) Granting Related Relief* [Docket No. 729].

6. Except as otherwise noted herein, the facts set forth in this declaration are based upon my personal knowledge and independent investigation, review of relevant Company policies, review of current and former versions of the Company's websites, including archived versions where available on the "waybackmachine" at www.archive.org, other information prepared by me or collected for me, and my conversations with the Company's counsel or other advisors.

7. If I were called to testify as a witness, I could and would competently testify to each of the facts set forth herein. I am over the age of eighteen and authorized to submit this declaration on behalf of the Company.

Transfer of Personally Identifiable Information Under the Bankruptcy Code

8. I understand that section 363 of the Bankruptcy Code permits a debtor to sell property of the estate and transfer "personally identifiable information about individuals to persons that are not affiliated with the debtor" when such transfer is consistent with the debtor's privacy policy in place as of the petition date. Further, I understand that the Bankruptcy Code requires the appointment of a consumer privacy ombudsperson when a debtor seeks to sell Personally Identifiable Information and such sale would be inconsistent with the debtor's privacy policy that is in effect on the petition date. *See* 11 U.S.C. §§ 332, 363(b)(1)(A). For the reasons set forth below, I conclude that any transfer of PHI and Personally Identifiable Information in connection with the Sale is consistent with the Company's privacy policies and would not necessitate the appointment of a consumer privacy ombudsperson.

The Company's Privacy Policies and Data Processing

9. The Company provides pharmaceutical services to long-term care facilities and post-acute care institutions across the United States. The Company collects certain personally

identifiable information[3] ("**Personally Identifiable Information**") and protected health information[4] ("**PHI**") to provide products and services to customers.

10. In its capacity as a pharmacy and provider of pharmacy-related services, the Company collects and processes both Personally Identifiable Information and PHI. The Company's data collection practices span five general categories, each governed by different privacy policies. The Company processes: (1) limited Personally Identifiable Information from general visitors to its public-facing websites, which is governed by the Company's Website Privacy Policy (as defined in ¶ 11, *infra*); (2) Personally Identifiable Information from users of the non-HIPAA covered portion of the MyOmniview Portal, which is governed by the MyOmniview Privacy Policy (as defined in ¶ 13, *infra*); (3) PHI from individuals who use MyOmniview portals associated with HIPAA-covered pharmacy services or otherwise interact with the Company's HIPAA-regulated offerings, which are governed by the Omnicare NPP (as defined in ¶ 13, *infra*); (4) Personally Identifiable Information from business-to-business individuals who use the Omniview Portal to manage or administer long-term care or facility-related operations, which is governed by the Omniview Privacy Policy (as defined in ¶ 16, *infra*); and (5) workforce-related Personally Identifiable Information from its employees, which is governed by the Workforce Privacy Policy (as defined in ¶ 18, *infra*). An accounting of the relevant privacy policies in effect on or prior to the Petition Date is attached as **Appendix 1**.

[3] Section 101(41A) of the Bankruptcy Code defines "personally identifiable information" to include (a) an individual's name, residential address, email address, phone number, Social Security number, or credit card number, as well as (b) an individual's date of birth or other information, that if associated with the information listed in (a), would permit the identification or contacting of the individual. 11 U.S.C. § 101(41A).

[4] HIPAA defines "protected health information" to mean any individually identifiable health information about a person's past, present, or future health, healthcare, or payment for healthcare, held by a "covered entity" or "business associate," in any format. 45 C.F.R. § 164.504. The Company's pharmacy business is a "covered entity" under HIPAA.

11. I tested the Company's data processing practices by (a) creating a "MyOmniview" account designed for service recipients; (b) signing up to receive email and SMS messages from the Company as part of the MyOmniview services;[5] (c) revoking my consent to receive email and SMS messages from the Company to confirm how the Company processes opt-out requests; (d) creating an "Omniview" account designed for facility managers; and (e) interacting with https://www.omnicare.com/ to assess how the Company's privacy policies and practices are incorporated into the Company's data collection and use from the consumer perspective.

12. The Company maintains a consumer-facing website at https://www.omnicare.com/ (the "**Omnicare Site**"). The Omnicare Site has a prominent link to the domain-level privacy policy (the "**Website Privacy Policy**"), applicable to Personally Identifiable Information of website visitors, in the footer of all Omnicare Site webpages. The Website Privacy Policy explains what information the Company collects about website visitors, how such data will be used and shared, the purposes of such data processing, and how website visitors can request the removal or modification of their data.

13. The Website Privacy Policy in effect on the Petition Date, and effective as of February 13, 2024,[6] provides in relevant part:

> *In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties,*

[5] Affirmative consent was required to receive pharmacy messages by email or SMS. The mechanics to withdraw such consent include unsubscribing to such emails or by replying "stop" to any text message. Each text message received from the Company included a reminder about the "stop" consent withdrawal mechanism.

[6] Although 11 U.S.C. § 363(b)(1)(A) is scoped to the privacy policy in effect on the petition date, I note that the Website Privacy Policy currently in effect (as of December 17, 2025) also contains language that is consistent with a sale of Personally Identifiable Information as part of the bankruptcy proceedings. *See* Omnicare, LLC, *Website Privacy Policy*, https://www.omnicare.com/privacy-policy/ (last visited May 1, 2026) ("In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation.").

> *personal information may be transferred to or shared with third parties as part of any such transaction or negotiation.*

See Website Privacy Policy, https://web.archive.org/web/20240803002521/https:/www.omnicare.com/privacy-policy/ (last visited May 1, 2026). A copy of this Website Privacy Policy is attached hereto as **Exhibit A**. A sale or transfer of Personally Identifiable Information to an unaffiliated third-party is expressly permitted under the Website Privacy Policy in effect as of the Petition Date.

14. The Company maintains the MyOmniview website for patients to access its services at https://myomniview.omnicare.com/ (the "**MyOmniview Portal**"). The MyOmniview Portal has a prominent link to the domain-level privacy policy (the "**MyOmniview Privacy Policy**"), applicable to Personally Identifiable Information of MyOmniview Portal visitors, and a Notice of Privacy Practices (the "**Omnicare NPP**"), that applies to PHI from individuals who use MyOmniview portals associated with HIPAA-covered pharmacy services or otherwise interact with the Company's HIPAA-regulated pharmacy offerings, in the footer of all Omnicare Site webpages. Both these privacy notices explain what information the Company collects about MyOmniview Portal visitors and pharmacy patients, how such data will be used and shared, the purposes of such data processing, and what rights individuals have with respect to their data.

15. The MyOmniview Privacy Policy in effect on the Petition Date, and effective as of October 31, 2022,[7] provides in relevant part:

> *In the event that Omnicare or some or all of our business, assets or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties,*

[7] Although 11 U.S.C. § 363(b)(1)(A) is scoped to the privacy policy in effect on the Petition Date, I note that the MyOmniview Privacy Policy currently in effect (as of January 8, 2026) also contains language that is consistent with a sale of Personally Identifiable Information as part of the bankruptcy proceedings. *See* Omnicare, LLC, *MyOmniview Privacy Policy,* https://myomniview.omnicare.com/PrivacyPolicy (last visited May 1, 2026) ("We may disclose your personal information to the following categories of recipients: . . . Other third parties: We may disclose your personal information to . . . (ii) relevant third parties (e.g., acquiring entity and its advisers) in the case of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of our business or assets.").

> *personal information may be transferred to or shared with third parties as part of any such transaction or negotiation.*

See MyOmniview Privacy Policy, https://web.archive.org/web/20230323175735/https:/myomniview.omnicare.com/PrivacyPolicy (last visited May 1, 2026), attached hereto as **Exhibit B**. A sale or transfer of Personally Identifiable Information to an unaffiliated third-party is expressly permitted under the MyOmniview Privacy Policy in effect as of the Petition Date.

16. The Omnicare NPP in effect on the Petition Date, and effective as of July 1, 2025, provides in relevant part:

> ***Health Care Operations:*** *We may use and disclose your PHI for health care operations – those activities necessary to operate our health care business. For example, we may: . . .*
>
> - *Transfer or receive your PHI if we buy or sell pharmacy locations.*

See Omnicare NPP, https://myomniview.omnicare.com/NoticeOfPrivacyPractices (last visited May 1, 2026), attached hereto as **Exhibit C**. A sale or transfer of PHI to an unaffiliated third-party is expressly permitted under the Omnicare NPP in effect as of the Petition Date, provided that, consistent with HIPAA, the buyer is or will become a HIPAA covered entity.

17. The Company maintains the Omniview website for facilities to manage the pharmacy services provided to patients at https://omniview.omnicare.com/na/apps/web/mvc/Login (the "**Omniview Portal**"). The Omniview Portal has a prominent link to the domain-level privacy policy (the "**Omniview Privacy Policy**"), applicable to Personally Identifiable Information of Omniview Portal users, in the footer of all Omnicare Site webpages. The Omniview Privacy Policy explains what information the Company collects about Omniview Portal users, how such data will be used and shared, the purposes of such data processing, and how users can request the removal or modification of their data.

18. The Omniview Privacy Policy in effect on the Petition Date, and effective as of October 31, 2022,[8] provides in relevant part: "In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation." *See Omniview Privacy Policy*, https://web.archive.org/web/20230418224825/https:/omniview.omnicare.com/na/apps/web/mvc/Public/PrivacyPolicy (last visited May 1, 2026), attached hereto as **Exhibit D**. A sale or transfer of Personally Identifiable Information to an unaffiliated third-party is expressly permitted under the Omniview Privacy Policy in effect as of the Petition Date.

19. The Company maintains a privacy policy applicable to the Personally Identifiable Information of its workforce members, which is accessible in the "Privacy Center" link included in the footer of the "Careers" webpage hosted by the Company's parent company, CVS Health, at https://jobs.cvshealth.com/us/en (the "**Workforce Privacy Policy**"). The Workforce Privacy Policy explains what information the Company collects about applicants and workforce members, how such data will be used and shared, the purposes of such data processing, and what rights individuals have with respect to their data.

[8] Although 11 U.S.C. § 363(b)(1)(A) is scoped to the privacy policy in effect on the Petition Date, I note that the Omniview Privacy Policy currently in effect (as of January 8, 2026) also contains language that is consistent with a sale of Personally Identifiable Information as part of the bankruptcy proceedings. *See* Omnicare, LLC, *Omniview Privacy Policy,* https://omniview.omnicare.com/na/apps/web/mvc/Public/PrivacyPolicy (last visited May 1, 2026) ("We may disclose your personal information to the following categories of recipients: . . . Other third parties: We may disclose your personal information to . . . (ii) relevant third parties (e.g., acquiring entity and its advisers) in the case of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of our business or assets.").

20. The Workforce Privacy Policy in effect on the Petition Date, and effective as of July 3, 2025,[9] provides in relevant part:

> ***3. How we use your personal information***
> *Depending on the nature of your relationship with us, we may use your personal information for the purposes listed below. . . .*
> - ***In connection with a sale or transfer of business assets.*** *To consider and implement mergers, acquisitions, reorganizations and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions. . . .*
>
> *We may disclose personal information for the following purposes:*
> - ***In connection with a sale or transfer of business assets.*** *We may disclose or transfer your personal information to other parties if some or all of our business, assets or stock are sold, transferred or used as security. This includes in connection with any bankruptcy or similar proceeding.*

See CVS Health, *Workforce Privacy Policy,* https://web.archive.org/web/20250724212404/https://www.cvshealth.com/privacy-policy/workforce.html (last visited May 1, 2026) attached hereto as

[9] The Workforce Privacy Policy currently in effect, and in effect as of October 10, 2025, includes supplemental policies for California residents (the "**CCPA Workforce Policy**") and non-US resident applicants (the "**International Recruitment Data Privacy Notice**"). Although 11 U.S.C. § 363(b)(1)(A) is scoped to the privacy policy in effect on the Petition Date, I note that these policies, and the currently-in-effect version of the Workforce Privacy Policy, also contain language that is consistent with a sale of Personally Identifiable Information as part of the bankruptcy proceedings. The Workforce Privacy Policy currently in effect states that "We may use your information . . . in connection with a sale or transfer of business assets." *See* CVS Health, *Workforce Privacy Policy,* https://www.cvshealth.com/privacy-policy/workforce.html (last visited May 1, 2026). The CCPA Workforce Policy states:

> In certain circumstances, we may disclose each category of your Personal Information to: . . . Relevant Third Parties as Part of a Corporate Transaction. In the event of a reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with a bankruptcy or similar proceeding), we may disclose or transfer your Personal Information to certain third parties, such as the acquiring entity and its advisers.

See CVS Health, *Workforce Privacy Policy,* https://www.cvshealth.com/privacy-policy/california-workforce-privacy-notice.html (last visited May 1, 2026). The International Recruitment Data Privacy Notice does not discuss transfers related to sales or corporate transactions, but states that it "supplements our Workforce Privacy Policy." *See* CVS Health, *Workforce Privacy Policy,* https://www.cvshealth.com/privacy-policy/international-recruitment-data-privacy-notice.html (last visited May 1, 2026).

Exhibit E. A sale or transfer of Personally Identifiable Information to an unaffiliated third-party is expressly permitted under the Workforce Privacy Policy in effect as of the Petition Date.

Sale or Transfer of PHI

21. The Omnicare NPP describes how the Company may use and disclose PHI for "healthcare operations" purposes, which includes in connection with the divestiture of pharmacy assets.[10] Such sale or transfer of PHI is subject to the HIPAA Privacy Rule and does not require affirmative patient consent so long as the acquiring company is a "covered entity" or will become one following the transaction.[11] Thus, provided that the sale occurs to a covered entity or a buyer that is or will become a covered entity following the transaction, the PHI transfer would be consistent with the Company's privacy policy and HIPAA.

22. Further, the Omnicare NPP provides that PHI may be used or disclosed for "healthcare operations" purposes, including, for example, to "[t]ransfer or receive your PHI if we buy or sell pharmacy locations," consistent with the HIPAA Privacy Rule.[12] *See* **Exhibit C**.

Sale or Transfer of Personally Identifiable Information

23. **Website Privacy Policy.** The Website Privacy Policy applicable to general visitors[13] to the Omnicare Site permits the transfer of Personally Identifiable Information to an

[10] "Healthcare operations" includes "the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity." *See* 45 C.F.R. § 164.506(c)(1).

[11] Covered entities are permitted to engage in such transactions with entities that are not covered entities, provided that the latter entity will become a covered entity following the transaction. *See* 45 C.F.R. § 164.501(6)(iv).

[12] *See* 45 C.F.R. § 164.506(c)(1); 65 Fed. Reg. 82,462, 82,491 (Dec. 28, 2000) (stating that the definition of health care operations includes "disclosure of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the transfer or sale is completed.").

[13] The Website Privacy Policy applies to only limited forms of personal information: contact information (such as name, phone number, and email address), survey responses, and data collected through cookies. "Personally identifiable information" subject to the Bankruptcy Code includes only the contact information and survey responses linked to an individual's name, phone number, or email address. *See* 11 U.S.C. § 101(41A).

unaffiliated third party as part of a corporate transaction or bankruptcy. *See* **Exhibit A**. Further, the Company informed consumers that use of the Omnicare Site constituted consent to the Website Privacy Policy. *See* **Exhibit A**. Thus, the transfer of such Personally Identifiable Information as part of a corporate transaction or bankruptcy is consistent with the Company's privacy policy that was in effect on the petition date.

24. **MyOmniview Privacy Policy.** The MyOmniview Privacy policy applicable to users of the non-HIPAA covered parts of the MyOmniview Portal permits the transfer of Personally Identifiable Information to unaffiliated third parties in connection with a corporate transaction or bankruptcy in its original version, effective September 15, 2017. *See* **Exhibit B**. Further, the Company informed consumers that creation of a MyOmniview Portal account and use of the MyOmniview Portal constituted consent to the MyOmniview Privacy Policy. *See* Omnicare, LLC, *MyOmniview Portal Account Registration,* https://myomniview.omnicare.com/Account/Register (last visited May 1, 2026); *see also* **Exhibit B**. Thus, the transfer of such Personally Identifiable Information as part of a corporate transaction or bankruptcy is consistent with the Company's privacy policy that was in effect on the petition date.

25. **Omniview Privacy Policy.** The Omniview Privacy Policy applicable to business and facility users permits the transfer of Personally Identifiable Information to unaffiliated third parties in connection with a corporate transaction or bankruptcy. *See* **Exhibit D**. Further, the Company informed business and facility users that use of the Omniview Portal constituted consent to the Omniview Privacy Policy. *See* **Exhibit D**. Thus, the transfer of such Personally Identifiable Information as part of a corporate transaction or bankruptcy is consistent with the Company's privacy policy that was in effect on the petition date.

26. **Workforce Privacy Policy.** The Workforce Privacy Policy applicable to Company employees, job applicants, former employees, contractors, and other workforce members permits the transfer of Personally Identifiable Information to unaffiliated third parties in connection with corporate transaction or bankruptcy. *See* **Exhibit E**. The Company informed employees, job applicants, former employees, contractors, and other workforce members that the processing of their Personally Identifiable Information is subject to the Workforce Privacy Policy. *See* **Exhibit E**. Thus, the transfer of such Personally Identifiable Information as part of a corporate transaction or bankruptcy is consistent with the Company's privacy policy that was in effect on the petition date.

27. Further, although the Company is subject to the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations (collectively, the "**CCPA**") with respect to workforce personal information, disclosures or transfers of personal information to third parties made as part of business transactions or transfers, such as mergers, acquisitions, or bankruptcy proceedings, are exempted from the definition of a "sale" of personal information.[14] As a result, sale-triggered obligations under the CCPA (i.e., opt-out rights) do not apply to the transfers related to this case.[15]

Conclusion

28. Based upon my investigation of the facts and circumstances surrounding the Company's collection and processing of PHI and Personally Identifiable Information, consumers were notified of and agreed to the transfer of their PHI and Personally Identifiable Information as

[14] *See* Cal. Civ. Code § 1798.140(ad).

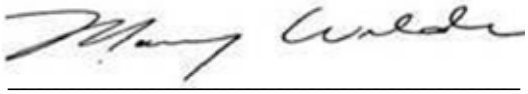
[15] If the buyer plans to use or disclose workforce personal information subject to the CCPA in a way that is materially inconsistent with the Workforce Privacy Policy, it must provide those workforce members with prior notice of the new or changed practice to the workforce member. Cal. Civ. Code § 1798.140(ad)(2)(C).

part of a sale or bankruptcy proceedings when they (a) subscribed to receive marketing communications; (b) registered for a MyOmniview Portal account; (b) used the Omnicare Site, MyOmniview Portal, or Omniview Portal; or (d) otherwise interacted with the Company, including in the employment context. I understand that the Company intends to conduct and complete the Sale of their assets in compliance with the terms of the applicable privacy policies. Accordingly, I believe that any transfer of PHI and Personally Identifiable Information in connection with such Sale would not necessitate the appointment of a consumer privacy ombudsperson.

* * * * *

29. Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing statements are true and correct to the best of my information and belief.

Dated: May 1, 2026



Marcy Wilder

Appendix 1:

Company Privacy Policies

Policy	Effective Date	Link	Exhibit	Bankruptcy Language
Website Privacy Policy	February 13, 2024	Archive	Exhibit A	"In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation."
MyOmniview Privacy Policy	October 31, 2022	Archive	Exhibit B	"In the event that Omnicare or some or all of our business, assets or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation."
Omniview Privacy Policy	October 31, 2022	Archive	Exhibit D	"In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation."
Omnicare NPP	July 1, 2025	Active	Exhibit C	"Health Care Operations: We may use and disclose your PHI for health care operations – those activities necessary to operate our health care business. For example, we may: . . . Transfer or receive your PHI if we buy or sell pharmacy locations."
Workforce Privacy Policy	July 3, 2025	Archive	Exhibit E	"We may use your personal information for the purposes listed below: … In connection with a sale or transfer of business assets. To consider and implement mergers, acquisitions, reorganizations and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions."

Exhibit A

Website Privacy Policy

The Wayback Machine - https://web.archive.org/web/20240803002521/https://www.omnicare.co...

Website
Privacy Policy

Effective Date: February 13, 2024

This Privacy Policy describes how Omnicare, Inc., a wholly owned subsidiary of CVS Health ("Omnicare," "we" or "us") may collect information about you through your interactions with us on www.omnicare.com and on our other websites and mobile applications (collectively, the "Services"). By using the Services, you agree to the terms of this Privacy Policy. If you have any questions or concerns about this Privacy Policy, or about the way your information is collected and used, please email us at webadministrator@omnicare.com.

This Privacy Policy does not apply to information that Omnicare collects about you on other Omnicare owned, operated, or sponsored websites that do not contain a link to this Privacy Policy or to the websites of Omnicare affiliates. In addition, this policy does not apply to the "Client Services" section of the Services, which is available only to certain Omnicare clients and is governed by separate agreements in place between Omnicare and its clients.

To the extent that information collected through the Services is patient information provided to obtain pharmacy services, this information is governed by the Omnicare Notice of Privacy Practices and not this Privacy Policy. If you have questions about which policy applies to information you have provided, please do not hesitate to contact us, or email us at webadministrator@omnicare.com.

We may change this Privacy Policy. The "Effective Date" legend at the top of this page indicates when this Privacy Policy was last revised. Any changes will become effective when we post the revised Privacy Policy on the Services. Your use of the Services following these changes means that you accept the revised Privacy Policy.

Who May Use the Services

We do not knowingly collect personal information online from any person we know to be under the age of 13, and we instruct users under 13 not to send any information to or through the Services.

The online Services are designed for users from, and are controlled and operated by us from, the United States. By using the Services, you consent to the transfer of your information to the United States or storage of your information in the United States, which may have different data protection rules than those of your country.

The Personal Information We Collect

We want you to understand how personal information you provide to us is collected and used. Personal information is any information that we can use to identify, locate, or contact you. We collect and store your personal information when you provide it to us or to our service providers. Some examples of personal information we collect and when we collect it include:

- **Registration**: We collect your personal information when you register on the Services.
- **Contact Information**: We collect personal information from users of the Services who are interested in receiving information about our products or services, such as prescription benefit, disease management, and specialty pharmacy services, e-mail alerts, newsletters, and other notifications.
- **Surveys**: From time to time, we request information from you via surveys. Participation in these surveys is voluntary. We request that you not provide personal health information in your survey responses. You may contact us regarding any survey as set forth under "Contact Information" below.

If you choose not to provide your personal information to us, we may not be able to provide you with requested products, services or information.

If you submit any personal information relating to other people in connection with the Services, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

We may combine the information collected from you through the Services with information we receive from and about you from other online and offline sources, and use

the combined information in accordance with this Privacy Policy.

Use and Disclosure of Personal Information

We may use personal information to personalize your experience on the Services, including by presenting products and content tailored to you, and for our business purposes, such as data analysis, audits, fraud monitoring and prevention, developing our Services and new products and services, determining the effectiveness of our promotional campaigns, and operating and expanding our business activities.

In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation.

To the extent permitted by applicable law, we may provide personal information to our affiliated businesses or to our business partners, who may use it to send you marketing and other communications.

We may disclose personal information to our service providers, who provide services such as website hosting, data analysis, information technology and related infrastructure provision, customer service, email delivery, auditing, and other services.

We may disclose your personal information to law enforcement officials as permitted or required by law. In matters involving claims of personal or public safety or in litigation where the information is pertinent (including to allow us to pursue available remedies or limit the damages that we may sustain), we may use or disclose personal information, including without court process. We may also use or disclose personal information to enforce our terms and conditions; to protect our operations or those of any of our affiliates; or to protect our rights, privacy, safety, or property and/or that of our affiliates, you, or others.

We may use and disclose personal information to investigate security breaches or otherwise cooperate with authorities pursuant to a legal matter.

We may use and disclose information that does not personally identify you (including the information described under “Cookies and Other Technologies” below) for any purpose, except to the extent limited by applicable law. If we are required to treat such information as personal information under applicable law, then we may use it for all the purposes for which we use and disclose personal information.

We may combine information that does not personally identify you with personal information. If we do, we will treat the combined information as personal information as

long as it is combined.

Social Media

We may use and disclose your personal information to facilitate social media sharing functionality that you initiate. If you choose to connect your social media account (e.g., Facebook, X, Pinterest) with your Services account or otherwise engage in social sharing on the Services, your personal information may be shared with your friends, contacts or others associated with your social media account; with other Services users; and with your social media account provider. By connecting your Services account and your social media account or contacting us via social media, you authorize us to share information with your social media account provider, and you understand that the use of the information we share will be governed by the social media site's privacy policy.

For example, if you utilize a social media feature such as the Facebook "Like" button, Google Plus, Pinterest or an X widget, these features may collect information about your IP address and which page you're visiting on our site, and they may set a cookie or employ other tracking technologies. Social media features and widgets are either hosted by a third party or hosted directly on our site. Your interactions with those features are governed by the privacy policies of the companies that provide them.

We may display targeted ads to you through social media platforms. These ads are sent to groups of people who share traits, such as where they live or have expressed an interest in shopping for cosmetics on our mobile site. We do not share any of your personally identifiable information, including your shopping history or health information, with social media platforms. See the policies of each social media platform for additional information about these types of ads, including how to manage your display settings for these ads.

Links

The Services may contain links to, or otherwise make available, third-party websites, services, or other resources not operated by us or on our behalf ("Third Party Services"). These links are provided as a convenience only and do not constitute an affiliation with, endorsement, or sponsorship of the Third Party Services. Any information you provide to such third parties is not subject to the terms of this Privacy Policy, and we are not responsible for the privacy or security of the information you provide to them or their handling of your information. We recommend that you review the privacy policy of any third party to whom you provide personal information online.

In addition, we are not responsible for the information collection, use, disclosure, or security policies and practices of other organizations, such as Apple, Google, Microsoft, RIM, or any other app developer, app provider, operating system provider, wireless service provider, or device manufacturer.

Information from Other Sources

We may collect data about you from publicly available sources to personalize your experience. We may also obtain data provided by third parties. For example, we may obtain information from companies to improve the accuracy of the information we have about you (e.g., adding your zip code to your address information). This improves our ability to contact you and increases the relevance of our offers and communications to you.

Security

We seek to use reasonable physical, technical, and administrative safeguards to protect personal information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account with us has been compromised), please immediately contact us in accordance with the “Contact Information” section below.

You are responsible for maintaining the confidentiality of your Services access information and password, and for restricting access to your device, and you agree to accept responsibility for all activities that occur under your password.

Telephone, Text, and Fax Policy

By providing your residential or wireless phone and/or fax number(s) to Omnicare, you expressly consent to receive marketing and non-marketing autodialed and/or prerecorded calls, text messages, and faxes (including fax advertisements) from or on behalf of Omnicare at the number(s) provided. Your consent to receive calls or texts on your wireless device is not a condition of any purchase. Consent may be revoked at any time by sending an opt-out request via email to webadministrator@omnicare.com with the phone and/or fax number you wish to opt-out. Your wireless carrier’s standard message and data rates may apply.

Text Messaging Terms & Conditions

Omnicare or one or more of its affiliates offers access to pharmacy and healthcare service messages via recurring SMS (Short Message Service), MMS (Multimedia Message Service) text alerts and email alerts. Enrollment in text alerts requires a member to provide his or her own mobile phone number with an area code within the 50 United States or the District of Columbia. Enrollment in email alerts requires member to provide an email address. By enrolling to receive Omnicare text or email alerts, you agree to these terms and conditions, which become effective upon your enrollment. You may be asked to verify your mobile phone number before the service will start. This requires responding to a text alert sent to your mobile phone confirming your enrollment in this Service.

You acknowledge that alerts will be sent to the mobile phone number or email address you provide to Omnicare. Such alerts may include limited personal information about your prescriptions, and whoever has access to the mobile phone or carrier account, or email address will also be able to see this information. Once you enroll, the frequency of text or email alerts we send to you will vary. You will typically receive alerts when we have information for you about your prescriptions or other healthcare information. Omnicare does not impose a separate charge for text alerts; however, your mobile carrier's message and data rates may apply depending on the terms and conditions of your mobile phone contract. You are solely responsible for all message and data charges that you incur. Please contact your mobile service provider about such charges. The following carriers are supported: AT&T, Sprint, Boost, Verizon Wireless, U.S. Cellular®, T-Mobile®, Cincinnati Bell, Alltel, Virgin Mobile USA, Cellular South, Unicel, Centennial, and nTelos.

You may opt out of Omnicare text alerts at any time. To stop receiving text alerts, text STOP to the number upon which you are receiving text alerts. Texting STOP to 53333, 68425 or 86053 (or the number you are receiving Omnicare alerts from) will opt you out of any and all future Omnicare text messages. After you submit a request to unsubscribe, you will receive one final text alert from Omnicare confirming that you will no longer receive text alerts. No additional text alerts will be sent unless you re-activate your enrollment to the text alert program. For questions about text alerts, text the word Help to 53333. Text alerts may come from any one of these short codes and Omnicare may change, add, or remove short codes as necessary.

The Omnicare text alert programs are offered on an "as is" basis and: (1) may not be available in all areas at all times; and (2) may not continue to work in the event of product, software, coverage, or other service changes made by your wireless carrier. Omnicare may change or discontinue any of its text alert programs without notice or liability to you. Omnicare and its related companies and each of their respective officers, directors, and employees are not responsible and shall not be liable for any losses or injuries of any kind resulting, directly or indirectly, from any Omnicare text alert program or from technical failures or delays of any kind. Omnicare reserves the right to cease delivery of text alerts to any person at any time in its sole discretion.

Cookies and Other Technologies

Like many other websites and online services, we collect information about the Services' traffic and usage patterns through the use of cookies, Web server logs, web beacons and other, similar technologies. We use this information for various purposes, such as to ensure that the Services function properly, to facilitate navigation, to personalize your experience, to understand use of the Services, to diagnose problems, to measure the success of our marketing campaigns and target advertisements, and to otherwise administer the Services.

Cookies are small computer files we transfer to your computer's hard drive. These small text files help us personalize content on our pages and provide programs. Your browser software can be set to reject or accept cookies. Instructions for resetting the browser are available in the Help section of most browsers.

Our use of cookies also allows us to collect and receive certain information about a website user, such as the type of Web browser used by our customer. Reviewing our Web server logs and our customers' use of our site helps us to, among other purposes, statistically monitor how many people are using our site and for what purpose.

Pixel tags are a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is open. Pixel tags are often used in combination with cookies.

Your IP address is a number that is automatically assigned to the computer that you are using by your Internet Service Provider. An IP address may be identified and logged automatically in our Web server log files whenever a user accesses the Services, along with the time of the visit and the page(s) visited. Collecting IP addresses is standard practice and is done automatically by many websites, applications, and other services. We use IP addresses for purposes such as calculating usage levels of the Services, helping diagnose server problems, and administering the Services.

Tracking / Third-Party Advertisers

We may use or partner third-party companies, including social medical companies like Facebook, as well as third-party advertising companies to provide measurements services and display targeted advertisements regarding goods and services that may be of interest to you when you access and use the Services; these targeted advertisements are based on information relating to your access to and use of the Services and of other online services. To do so, these companies may place or recognize a unique cookie on your browser including through the use of pixel tags, web beacons, and other storage technologies to collect or receive information from our website and elsewhere on the internet. We may use analytics providers that use cookies, pixel tags, web beacons, and other, similar technologies to collect or receive information about your use of the Services and your use of other websites or online services.

You may opt out of the collection and use of information for advertisement targeting, at any time. To acquire further information and exercise your right to opt out you may defer to consumer choice tools created under self-regulation programs, such as http://www.networkadvertising.org/managing/opt_out.asp and https://youradchoices.com. Note: Even if you opt out of targeted advertisements, you may still see or receive other types of online advertising based on factors such as general location derived from your IP address, your browser type, and your search terms.

Lastly, you may manage cookies in your web browser. Your browser software can be set to reject or accept cookies. Instructions for resetting the browser are available in the Help section of most browsers.

We do not respond to browser do-not-track signals.

Physical Location

We and our service providers may collect the physical location of your device by, for example, using satellite, cell phone tower, WiFi signals, beacons, Bluetooth, and near field communication protocols, when you are in or near a CVS store. We may use your device's physical location to provide you with personalized location-based services and content, including for marketing purposes. We may also use such information to understand traffic patterns in, near, and across our store locations. We may share aggregated statistics derived from the location and other information we collect with advertisers and other third parties. You may be permitted to allow or deny such collection of your device's location, such as through the settings on your mobile device and/or, to avoid the collection of location by beacons, by disabling Bluetooth. If you choose to deny such collection, we and our service providers may not be able to provide you with certain personalized services and content.

For example, precise geo-location can be used to identify your device's latitude and longitude or your device's location capability (e.g., GPS or Wi-Fi) to help you find nearby CVS stores. Or, in-store location through the use of your phone's Bluetooth signal, LED light chip technologies, or other technologies will permit CVS to provide additional services to you.

Fraudulent Sites, Spam & Phishing

Please be aware that there may be fraudulent websites that illegally use Omnicare logos and other aspects of the Omnicare brand. Omnicare is in no way associated with any fraudulent websites. These sites may circulate their presence on the internet via spam email or through fraudulent phishing practices.

These sites have not been authorized by Omnicare to use our name, and we work aggressively to identify their source and have them shut down. If you are in receipt of this type of spam email, to help protect your privacy you should avoid replying to it or forwarding it to other people.

In addition to our official websites, Omnicare works with a number of third parties that host websites and micro-sites that provide information and services to our customers. If you are concerned that a website or an email may be fraudulent, please email us at webadministrator@omnicare.com.

Your Choices and Access

You can request the removal or modification of the personal information you have provided to us by sending an email to the appropriate area under “Contact Us.” For your protection, we may only implement requests with respect to the personal information associated with the particular email address that you use to send us your request, and we may need to verify your identity and obtain information on the context in which you provided your personal information before implementing your request. We will try to accommodate your request as soon as reasonably practicable.

You can stop all further collection of information by an Omnicare mobile application by uninstalling the Omnicare mobile application. You may use the standard uninstall process available as part of your mobile device or via the mobile application marketplace or network.
Note: If you uninstall the mobile application from your device, the Omnicare unique identifier associated with your install and/or device might continue to be stored. If you re-install the application on the same device, Omnicare might be able to re-associate this identifier to your previous transactions and activities.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting such change or deletion. There may also be residual information that will remain within our databases and other records, which will not be removed.

Your California Privacy Rights

If you are our customer and a California resident, you may request that we provide you with certain information about the entities with which we have shared our customers’ personal information for direct marketing purposes during the preceding calendar year. To do so, please write to us at ConsumerPrivacy@cvshealth.com.

Contact Information

If you have any questions about the content of this Privacy Policy, please contact us at web administrator@omnicare.com or the CVS Health Privacy Office at the following address:

CVS Health
Attn: Privacy Office
One CVS Drive
Woonsocket, R.I. 02895
1-888-607-4287

Request a Consultation

Get in touch and schedule a consultation today. You can change this!

Request a Consultation

Connect with us

Request a Consultation

Overview
Expertise and Support
Value and Services
Making the Switch
Overview
Pharmacy Management Systems
Packaging and Medication
Predictive Refill Programs
Overview
Clinical Pharmacy Consulting
Transition of Care
Clinical Intervention Center
Infusion Services and Education

CAREERS

©2024 Omnicare® a CVS Health Company

Sitemap
Privacy Policy
Accessibility
CVS Health Code of Conduct
Terms of Use

Exhibit B

MyOmniview Privacy Policy

The Wayback Machine - https://web.archive.org/web/20230323175735/https://myomniview.omnicare.com/PrivacyPolicy

MyOmniview

Back to sign in

Privacy Policy

Effective Date: October 31, 2022

This Privacy Policy describes how Omnicare, Inc., a wholly owned subsidiary of CVS Health ("Omnicare," "we" or "us") may collect information about you through your interactions with us on https://myomniview.omnicare.com/ and on our other websites and mobile applications (collectively, the "MyOmniview Portal"). By using the MyOmniview Portal, you agree to the terms of this Privacy Policy. If you have any questions or concerns about this Privacy Policy, or about the way your information is collected and used, please call us toll-free at **1-855-LET-OMNI (538-6664)** 1-855-LET-OMNI (538-6664).

To the extent that information collected through the MyOmniview Portal is patient information provided to obtain pharmacy services, this information is governed by the Omnicare Notice of Privacy Practices and not this Privacy Policy. If you have questions about which policy applies to information you have provided, please do not hesitate to Contact Us, or call us toll-free at **1-855-LET-OMNI (538-6664)** 1-855-LET-OMNI (538-6664).

We may change this Privacy Policy. The "Effective Date" legend at the top of this page indicates when this Privacy Policy was last revised. Any changes will become effective when we post the revised Privacy Policy on the MyOmniview Portal. Your use of the MyOmniview Portal following these changes means that you accept the revised Privacy Policy.

Who May Use the Services

We do not knowingly collect personal information online from any person we know to be under the age of 13 and instruct users under 13 not to send us any information to or through the MyOmniview Portal.

The MyOmniview Portal is designed for users from, and are controlled and operated by us from, the United States. By using the MyOmniview Portal, you consent to the transfer of your information to the United States or storage of your information in the United States, which may have different data protection rules than those of your country.

The Personal Information We Collect

We want you to understand how personal information you provide to us is collected and used. Personal information is any information that we can use to identify, locate, or contact you. We may collect and store your personal information when you provide it to us or to our service providers. Some examples of personal information we collect and when we collect it include:

- when you register for accounts on our website or mobile applications

- when you contact Omnicare for support
- when you participate in surveys
- when you indicate that you are interested in receiving information about our products or services, such as e-mail alerts, newsletters, and other notifications
- how you use our sites and mobile applications, search terms, pages you visit on our mobile applications, computer and mobile device information and push notification services you request
- when you purchase an item from us we will collect your financial information, such as your credit or debit card information, to process the payment

If you choose not to provide your personal information to us, we may not be able to provide you with requested products, services or information.

If you submit any personal information relating to other people in connection with the MyOmniview Portal, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

We may combine the information collected from you through the MyOmniview Portal with information we receive from and about you from other online and offline sources and use the combined information in accordance with this Privacy Policy. Our goal is to offer you content, advertisements, products, and services that are most likely to appeal to you.

Use and Disclosure of Personal Information

We use your personal information to respond to your requests, such as to fulfill your order, contact you with information about your order, send you email alerts, send you newsletters, and to provide you with related customer service. We may also use your information to send marketing communications and administrative information to you. Manage subscription services, including order management, billing, improving reorder experiences, communicate with you about your account, and offer other products and services that may be of interest to you.

We may use your personal information to personalize your experience and interacting with us, including by presenting products and offers tailored to you, and for our business purposes, such as data analysis, audits, fraud monitoring and prevention, developing the MyOmniview Portal and new products and services, determining the effectiveness of our promotional campaigns, and operating and expanding our business activities.

In the event that Omnicare or some or all of our business, assets or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation.

To the extent permitted by applicable law, we may provide personal information to our affiliated businesses or to our business partners, who may use it to send you marketing and other communications.

We may disclose personal information to our service providers, who provide services such as website hosting, data analysis, payment processing, order fulfilment, information technology and related infrastructure provision, customer service, email delivery, auditing, and other services.

If we are requested by law enforcement officials or judicial authorities to provide personal information, we may do so. In matters involving claims of personal or public safety or in litigation where the information is pertinent (including to allow us to pursue available remedies or limit the damages that we may sustain), we may use or disclose personal information, including without court process. We may also use or disclose personal information to enforce our terms and conditions, to protect our operations or those of any of our affiliates, or to protect our rights, privacy, safety or property and/or that of our affiliates, you, or others.

We may use and disclose personal information to investigate security breaches or otherwise cooperate with authorities pursuant to a legal matter.

We may use and disclose information that does not personally identify you (including the information described under "Cookies and Other Technologies," below) for any purpose, except to the extent limited by applicable law. If we are required to treat such information as personal information under applicable law, then we may use it for all the purposes for which we use and disclose personal information.

We may combine information that does not personally identify you with personal information. If we do, we will treat the combined information as personal information as long as it is combined.

Links

The MyOmniview Portal may contain links to, or otherwise make available, third-party websites, services, or other resources not operated by us or on our behalf ("Third Party Services"). These links are provided as a convenience only and do not constitute an affiliation with, endorsement or sponsorship of the Third Party Services. Any information you provide to such third parties is not subject to the terms of this Privacy Policy, and we are not responsible for the privacy or security of the information you provide to them or their handling of your information. We recommend that you review the privacy policy of any third party to whom you provide personal information online.

In addition, we are not responsible for the information collection, use, disclosure, or security policies and practices of other organizations, such as Apple, Google, Microsoft, RIM, or any other app developer, app provider, operating system provider, wireless service provider, or device manufacturer.

Information from Other Sources

We may collect data about you from publicly available sources to personalize your experience. We may also obtain data provided by third parties. For example, we may obtain information from companies to improve the accuracy of the information we have about you (e.g., adding your zip code to your address information). This improves our ability to contact you and increases the relevance of our offers and communications to you.

Security

We seek to use reasonable physical, technical, and administrative safeguards to protect personal information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account with us has been

compromised), please immediately contact us in accordance with the "Contact Information" section below.

You are responsible for maintaining the confidentiality of your MyOmniview Portal access information and password and for restricting access to your device, and you agree to accept responsibility for all activities that occur under your password.

Telephone, Text and Fax Policy

By providing your residential or wireless phone and/or fax number(s) to Omnicare, you expressly consent to receive marketing and non-marketing autodialed and/or prerecorded calls, text messages and faxes (including fax advertisements) from or on behalf of Omnicare at the number(s) provided. Your consent to receive calls or texts on your wireless device is not a condition of any purchase. Consent may be revoked at any time by calling the toll-free number at **1-877-265-2711** 1-877-265-2711 or faxing your opt-out request to **1-401-652-0893** 1-401-652-0893. You may also send an opt-out request via email to do_not_call@cvscaremark.com with the phone and/or fax number you wish to opt-out. Your wireless carrier's standard message and data rates may apply.

Text Messaging Terms and Conditions

Omnicare or one or more of its affiliates offers access to pharmacy and healthcare service messages via recurring SMS (Short Message Service) and MMS (Multimedia Message Service) text alerts. Enrollment in text alerts requires a patient to provide his or her own mobile phone number with an area code within the 50 United States or the District of Columbia. By enrolling to receive Omnicare text alerts, you agree to these terms and conditions, which become effective upon your enrollment. You may be asked to verify your mobile phone number before the service will start. This requires responding to a text alert sent to your mobile phone confirming your enrollment in this Service.

You acknowledge that text alerts will be sent to the mobile phone number you provide to Omnicare. Such alerts may include limited personal information about your prescriptions, and whoever has access to the mobile phone or carrier account will also be able to see this information. Once you enroll, the frequency of text alerts we send to you will vary. You will typically receive text alerts when we have information for you about your prescriptions or other healthcare information. Omnicare does not impose a separate charge for text alerts; however, your mobile carrier's message and data rates may apply depending on the terms and conditions of your mobile phone contract. You are solely responsible for all message and data charges that you incur. Please contact your mobile service provider about such charges. The following carriers are supported: AT&T;, Sprint, Boost, Verizon Wireless, U.S. Cellular®, T-Mobile®, Cincinnati Bell, Alltel, Virgin Mobile USA, Cellular South, Unicel, Centennial and nTelos. You may opt out of MyOmniview text alerts at any time. To stop receiving text alerts, text STOP to MYOMVW (696689). Texting STOP to MYOMVW (696689) will opt you out of any and all future MyOmniview text messages. After you submit a request to unsubscribe, you will receive one final text alert from MyOmniview confirming that you will no longer receive text alerts. No additional text alerts will be sent unless you re-activate your enrollment. For questions about text alerts, text the word HELP to MYOMVW (696689) or contact MyOmniview at **1-877-265-2711**1-877-265-2711. You also can change your text alert preferences on Omnicare.com if you have an account with prescription management. Sign in and go to your pharmacy main page. Click on the On/Off button in the Pharmacy Messages section to change your preferences.

The Omnicare text alert programs are offered on an "as is" basis and: (1) may not be available in all areas at all times; and (2) may not continue to work in the event of product, software, coverage or other service changes made by your wireless carrier. Omnicare may change or discontinue any of its text alert programs without notice or liability to you. Omnicare and its related companies and each of their respective officers, directors and employees are not responsible and shall not be liable for any losses or injuries of any kind resulting, directly or indirectly, from any Omnicare text alert program or from technical failures or delays of any kind. Omnicare reserves the right to cease delivery of text alerts to any person at any time in its sole discretion.

Cookies and Other Technologies

Like many other websites and online services, we collect information about the MyOmniview Portal's traffic and usage patterns through the use of cookies, Web server logs, web beacons and other, similar technologies. We use this information for various purposes, such as to ensure that the MyOmniview Portal function properly, to facilitate navigation, to personalize your experience, to understand use of the MyOmniview Portal, to diagnose problems, to measure the success of our marketing campaigns, and to otherwise administer the MyOmniview Portal.

Cookies are small computer files we transfer to your computer's hard drive. These small text files help us personalize content on our pages. Your browser software can be set to reject or accept cookies. Instructions for resetting the browser are available in the Help section of most browsers.

Our use of cookies also allows us to collect and receive certain information about a website user, such as the type of Web browser used by our customer. Reviewing our Web server logs and our customers' use of our site helps us to, among other purposes, statistically monitor how many people are using our site and for what purpose.

Pixel tags are a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is open. Pixel tags are often used in combination with cookies.

Your IP address is a number that is automatically assigned to the computer that you are using by your Internet Service Provider. An IP address may be identified and logged automatically in our Web server log files whenever a user accesses the MyOmniview Portal, along with the time of the visit and the page(s) that were visited. Collecting IP addresses is standard practice and is done automatically by many websites, applications and other services. We use IP addresses for purposes such as calculating usage levels of the MyOmniview Portal, helping diagnose server problems, and administering the MyOmniview Portal.

We may use Adobe Flash Local Stored Objects ("LSOs") and other technologies to, among other things, collect and store information about your use of the MyOmniview Portal. If you do not want Flash LSOs stored on your computer, you can adjust the settings of your Flash player to block Flash LSO storage using the tools contained in the Website Storage Settings Panel. You can also control Flash LSOs by going to the Global Storage Settings Panel and following the instructions (which may include instructions that explain, for example, how to delete existing Flash LSOs (referred to "information" on the Macromedia site), how to prevent Flash LSOs from being placed on your computer without your being asked, and (for Flash Player 8 and later) how to block Flash LSOs that are not being delivered by the operator of the page you are on at the time). Please note that setting

the Flash Player to restrict or limit acceptance of Flash LSOs may reduce or impede the functionality of some Flash applications.

Tracking/Third-Party Advertisers

We may use or partner third-party companies, including social media companies like Facebook, as well as third-party advertising companies to provide measurements services and display targeted advertisements regarding goods and services that may be of interest to you when you access and use the MyOmniview Portal; these targeted advertisements are based on information relating to your access to and use of the MyOmniview Portal and of other online services. To do so, these companies may place or recognize a unique cookie on your browser including through the use of pixel tags, web beacons, and other storage technologies to collect or receive information from our website and elsewhere on the internet. We may use analytics providers that use cookies, pixel tags, web beacons, and other, similar technologies to collect or receive information about your use of the MyOmniview Portal and your use of other websites or online services.

You may opt out of the collection and use of information for advertisement targeting, at any time. To acquire further information and exercise your right to opt out you may defer to consumer choice tools created under self-regulation programs, such as http://www.networkadvertising.org/managing/opt_out.asp and http://www.aboutads.info/.

. **Note: Even if you opt out of targeted advertisements, you may still see or receive other types of online advertising based on factors such as general location derived from your IP address, your browser type, and your search terms.**
Lastly, you may manage cookies in your web browser. Your browser software can be set to reject or accept cookies. Instructions for resetting the browser are available in the Help section of most browsers.

We do not respond to browser do-not-track signals.

Fraudulent Sites, Spam & Phishing

Please be aware that there may be fraudulent websites that illegally use Omnicare logos, and other aspects of the Omnicare brand. Omnicare is in no way associated with any fraudulent websites. These sites may circulate their presence on the internet via spam email, or through fraudulent phishing practices.

These sites have not been authorized by Omnicare to use our name and we work aggressively to identify their source and have them shut down. If you are in receipt of this type of spam email, to help protect your privacy you should avoid replying to it or forwarding it to other people.

In addition to our official websites, Omnicare works with a number of third parties that host websites and micro-sites that provide information and services to our customers. If you are concerned that a website or an email may be fraudulent, please contact us by phone at **855-LET-OMNI (538-6664)** 855-LET-OMNI (538-6664) with your concerns.

Your Choices and Access

You can take yourself off our email list for promotional offers at any time by updating your Email Communications preference in your Account Profile in the My Account section or by following the instructions contained in such emails. If you opt out of receiving promotional emails from us, we may still send you important administrative messages, from which you cannot opt out.

You can request the removal or modification of the personal information you have provided to us by sending an email to the appropriate area under "Contact Us". For your protection, we may only implement requests with respect to the personal information associated with the particular email address that you use to send us your request, and we may need to verify your identity and obtain information on the context in which you provided your personal information before implementing your request. We will try to accommodate your request as soon as reasonably practicable.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting such change or deletion. There may also be residual information that will remain within our databases and other records, which will not be removed.

Your California Privacy Rights

If you are our customer and a California resident, you may request that we provide you with certain information about the entities with which we have shared our customers' personal information for direct marketing purposes during the preceding calendar year. To do so, please write to us ConsumerPrivacy@cvshealth.com.

Deidentified Patient Information

In addition to personal information, we may sell or disclose patient and/or member information that has been deidentified as permitted by law. To the extent we sell or share such deidentified patient and/or member information, we do so pursuant to one of the deidentification methodologies described in Section 164.514(b)(1) or (b)(2) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method and the HIPAA safe harbor method, respectively.

Your Responsibility

By establishing a MyOmniview Portal account, you agree that it is your responsibility to:

- Authorize, monitor, and control access to and use of your https://myomniview.omnicare.com/ account, User ID and password.
- Promptly inform us of any need to deactivate a password or an account by calling **855-LET-OMNI (538-6664)** 855-LET-OMNI (538-6664)

Contact Information

If you have any questions or concerns about this statement, or about the way your information is collected and used, please Contact Us or call us toll-free at **855-LET-OMNI (538-6664)** 855-LET-OMNI (538-6664).

If you have any questions about the content of this Privacy Policy, please contact us at webadministrator@omnicare.com or the CVS Health Privacy Office at the following address:

CVS Health
Attn: Privacy Office
One CVS Drive
Woonsocket, R.I. 02895
1-888-607-4287

Back to sign in

Review our Privacy Policy, Notice of Privacy Practices, Terms of Use and Non-Discrimination Policies | Contact Us | FAQs

Copyright © 2023 Omnicare, Inc.

Privacy Policy | Notice of Privacy Practices

Terms of Use | Non-Discrimination Policies

Contact Us | FAQs

Copyright © 2023 Omnicare, Inc.

20230113.5

Exhibit C

Omnicare NPP

Notice of Privacy Practices

Effective Date: July 1, 2025

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.

This Notice of Privacy Practices (the "Notice") describes the privacy practices of Omnicare, Inc. ("Omnicare") and the members of its Affiliated Covered Entity ("CVS Provider ACE"). An Affiliated Covered Entity is a group of Covered Entities under common ownership or control that designates itself as a single Covered Entity for purposes of compliance with the Health Insurance Portability and Accountability Act ("HIPAA"). The members of the CVS Provider ACE will share Protected Health Information ("PHI") with each other for the treatment, payment, and health care operations of the CVS Provider ACE and as permitted by HIPAA and this Notice. For a complete list of the members of the CVS Provider ACE, please contact the CVS Health Privacy Office.

PHI is information about you that we obtain to provide our services to you and that can be used to identify you. It includes your name and contact information, as well as information about your health, medical conditions and prescriptions. It may relate to your past, present or future physical or mental health or condition, the provision or health care products and services to you, or payment for such products or services.

We are required by law to protect the privacy of your PHI and to provide you with this Notice explaining our legal duties and privacy practices regarding your PHI. This Notice describes how we may use and disclose your PHI. We have provided you with examples; however, not every permissible use or disclosure will be listed in this Notice. PHI disclosed

as permitted by HIPAA may be subject to redisclosure by the recipient and no longer protected by HIPAA. This Notice also describes your rights and the obligations we have regarding the use and disclosure of your PHI. We and our employees and workforce members are required to follow the terms of this Notice or any change to it that is in effect.

Uses and Disclosures of Your PHI for Treatment, Payment and Health Care Operations

We may use and disclose your PHI for treatment, payment and health care operations without your written authorization. The following categories describe and provide some examples of the different ways that we may use and disclose your PHI for these purposes:

Treatment: We may use and disclose your PHI to provide and coordinate the treatment, medication and services you receive. For example, we may:

- Use and disclose your PHI to provide and coordinate the treatment, medication and services you receive from Omnicare.
- Disclose your PHI to other third parties, such as pharmacies, doctors, hospitals, care facilities or other health care providers to assist them in providing care to you or for care coordination. In some instances, uses and disclosures of your PHI for these purposes may be made through a Health Information Exchange or similar shared system.
- Contact you to provide treatment-related services, such as refill reminders, adherence communications, or treatment alternatives (e.g., available generic products).

Payment: We may use and disclose your PHI to obtain payment for the services we provide to you and for other payment activities related to the services we provide. For example, we may:

- Share your PHI with your insurer, pharmacy benefit manager, or other health care payor to determine whether it will pay for the health care products and services you need or receive from us and to determine the payment amount you may owe.
- Contact you about a payment or balance due for prescriptions dispensed to you by Omnicare.
- Disclose your PHI to other health care providers, including care facilities, health plans or other HIPAA Covered Entities who may need it for their payment activities.

Health Care Operations: We may use and disclose your PHI for health care operations – those activities necessary to operate our health care business. For example, we may:

- Use and disclose your PHI to monitor the quality of our health care services, to provide customer services to you, to resolve complaints, and to coordinate your care.
- Transfer or receive your PHI if we buy or sell pharmacy locations.
- Use and disclose your PHI to contact you about health-related products, services or opportunities that may interest you, such as programs for our patients.
- Disclose your PHI to other HIPAA Covered Entities that have provided services to you so that they can improve the quality and efficacy of the health care services they provide or for their health care operations.
- Use your PHI to create de-identified data, which no longer identifies you, and which may use or disclosed for analytics, business planning or other purposes.

Other Uses and Disclosures of Your PHI that Do Not Require Authorization

We are also allowed or required to share your PHI, without your authorization, in certain situations or when certain conditions have been met.

Business Associates: When we contract with third parties to perform certain services for us, such as billing or consulting, these third-party service providers, known as Business Associates, may need access to your PHI to perform these services. They are required by law and their agreements with us to protect your PHI in the same way we do.

Individuals Involved in Your Care or Payment for Your Care: We may disclose your PHI to a friend, personal representative, family member, or any other person you identify as a caregiver, who is involved in your care or the payment related to that care. For example, we may provide prescriptions and related information to your caregiver on your behalf. We may also make these disclosures after your death unless doing so is inconsistent with any prior expressed preference documented by Omnicare. Upon your death, we may disclose your PHI to an administrator, executor, or other individual authorized under law to act on behalf of your estate. If you are a minor, we may release your PHI to your parents or legal guardians when permitted or required by law.

Workers' Compensation: We may disclose your PHI as necessary to comply with laws related to workers' compensation or similar programs.

Law Enforcement: We may disclose your PHI to law enforcement officials as permitted or required by law. For example, we may use or disclose your PHI to report certain injuries or to report criminal conduct that occurred on our premises. We may also disclose your PHI in response to a court order, subpoena, warrant, or other similar written request from law enforcement officials.

Required by Law: We will disclose your PHI when required to do so to comply with federal, state or local law.

Judicial and Administrative Proceedings: We may disclose your PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process.

Public Health and Safety Purposes: We may disclose your PHI in certain situations to help with public health and safety issues when we are required or permitted to do so, for example to: prevent disease; report adverse reactions to medications; report suspected abuse, neglect or domestic violence; or to prevent or reduce a threat to anyone's health or safety.

Health Oversight Activities: We may disclose your PHI to an oversight agency for certain activities including audits, investigations, inspections, licensure or disciplinary actions, or civil, administrative, and criminal proceedings, and as necessary for oversight of the health care system, government programs, or compliance with civil rights laws.

Research: Under certain circumstances, we may use or disclose your PHI for research purposes. For example, we may use or disclose your PHI as part of a research study when the research has been approved by an institutional review board and there is an established protocol to ensure the privacy of your information.

Coroners, Medical Examiners and Funeral Directors: We may disclose PHI to coroners, medical directors, or funeral directors so that they can carry out their duties.

Organ or Tissue Donation: We may disclose your PHI to organ procurement organizations.

Notification: We may use or disclose your PHI to notify or assist in notifying a family member, personal representative, or any other person responsible for your care regarding your location, general condition, or death. We may also disclose your PHI to disaster relief organizations so that your family or other persons responsible for your care can be notified of your location, general condition, or death.

Correctional Institution: If you are or become an inmate of a correctional institution, we may disclose your PHI to the institution or its agents to assist them in providing your health care, protecting your health and safety or the health and safety of others.

Specialized Government Functions: We may disclose your PHI to authorized federal officials for the conduct of military, national security activities and other specialized government functions.

Uses or Disclosures for Purposes that Require Your Authorization

Use and disclosure of your PHI for other purposes may be made only with your written authorization and unless we have your authorization we will not:

- Use or disclose your PHI for marketing purposes.
- Share psychotherapy notes (to the extent we have any).
- Sell your PHI to third parties (except for in connection with the transfer of a business to another health care provider required to comply with HIPAA).

We will obtain your written authorization before using or disclosing your PHI for purposes other than those described in this Notice or otherwise permitted by law. You may revoke your authorization at any time by submitting a written notice to the CVS Health Privacy Office. Your revocation will be effective upon receipt; however, it will not undo any use or disclosure of your PHI that occurred before you notified us, or any actions taken based upon your authorization..

Additional Restrictions on Use and Disclosure

Some state and federal laws may require special privacy protections, including certain requirements to obtain attestations from requestors, that limited the use and disclosure of certain sensitive health information. Such laws may protect information related to:

- Alcohol or substance use disorder
- Biometric Information
- Child or adult abuse or neglect, including sexual assault
- Communicable diseases
- Genetic information
- HIV/AIDs
- Mental health
- Minors
- Reproductive health
- Sexually transmitted diseases

We will follow the law that is stricter (or more protective of your PHI), where it applies to us. If you would like additional information about additional use or disclosure restrictions that may apply to your sensitive PHI, please contact the CVS Health Privacy Office

Your Health Information Rights

Written Requests and Additional Information: you may request additional information about Omnicare's privacy practices or obtain forms for submitting written requests by contacting the **CVS Health Privacy Officer**: by email at **PrivacyOffice@CVSHealth.com**, by mail at **CVS Health Privacy Office, One CVS Dr., Woonsocket RI 02895** or toll-free by telephone at **(833) 571-1784**. You can also visit **www.omnicare.com** to obtain the forms to submit written requests.

Obtain a Copy of the Notice: You have the right to obtain a paper copy of our current Notice at any time. You may do so by going to the site where you obtain health care services from us or by contacting the CVS Health Privacy Office.

Inspect and Obtain a Copy of Your PHI: With a few exceptions, you have the right to see and get a copy of the PHI we maintain about you. You may request access to your PHI electronically. To inspect or obtain a copy of your PHI, submit a written request to the CVS Health Privacy Office. You may also ask us to provide a copy of your PHI to another person or entity. A reasonable fee may be charged for the expense of fulfilling your request as permitted under HIPAA and/or state law. We may deny your request to inspect and copy your record in certain limited circumstances. If we deny your request, we will notify you in writing and let you know if you may request a review of the denial.

Request an Amendment: If you feel that the PHI we maintain about you is incomplete or incorrect, you may request that we amend it. For example, if your date of birth is incorrect, you may request that the information be corrected. To request an amendment, submit a written request to the CVS Health Privacy Office. You must include a reason that supports your request. If we deny your request for a n amendment, we will provide with you a written explanation of why we denied it.

Receive an Accounting of Disclosures: You have the right to request an accounting of disclosures we make of your PHI for purposes other than treatment, payment, or health care operations. Please note that certain other disclosures need not be included in the accounting we provide to you. To obtain an accounting, submit a written request to the CVS Health Privacy Office. We will provide one accounting per 12 -month period free of charge, but you may be charged for the cost of any subsequent accountings. We will notify you in advance of the cost involved, and you may choose to withdraw or modify your request at that time.

Request Confidential Communications: You have the right to request that we communicate with you in a certain way or at a certain location. For example, you may request that we contact you only in writing at a specific address. To request confidential communication of your PHI, submit a written request to the CVS Health Privacy Office.

Your request must state how, where, or when you would like to be contacted. We will accommodate all reasonable requests.

Request a Restriction on Certain Uses and Disclosures: You have the right to request additional restrictions on our use and disclosure of your PHI by sending a written request to the CVS Health Privacy Office. We are not required to agree to your request except where the disclosure is to a health plan or insurer for purposes of carrying out payment or health care operations, is not otherwise required by law, and the PHI is related to a health care item or service for which you, or a person on your behalf, has paid in full out-of-pocket. If you do not want a claim for payment submitted to your health plan on record, please discuss with the pharmacist or health care provider when you check in for care or before your prescription is sent to the pharmacy.

Notification of Breach: You have a right to be notified in the event there is a breach of your unsecured PHI as defined by HIPAA.

To report a problem

Complaints: If you believe your privacy rights have been violated, you can file a complaint with the CVS Health Privacy Officer or with the Secretary of the United States Department of Health and Human Services. All complaints must be submitted in writing. **You will not be penalized or otherwise retaliated against in any way for filing a complaint.**

Changes to this notice

We reserve the right to make changes to this Notice as permitted by law and to make the revised Notice effective for PHI we already have about you as well as any information we receive in the future, as of the effective date of the revised Notice. If we make material or important changes to our privacy practices, we will promptly revise our Notice. Upon request to the Privacy Office, Omnicare will provide a revised Notice to you. We will also post the revised Notice in our physical locations where we provide Omnicare services and on our Web site at **https://www.omnicare.com/notice-of-privacy-practices/** and will make copies available at our direct treatment facilities.

Effective Date. This Notice is effective as of July 1, 2025.

Request a Consultation

Get in touch and schedule a consultation today.

Request a Consultation

Connect with us

- Overview
- Expertise and Support
- Value and Services
- Making the Switch
- Overview
- Pharmacy Management Systems
- Packaging and Medication
- Predictive Refill Programs
- Overview
- Clinical Pharmacy Consulting
- Transition of Care
- Clinical Intervention Center
- Infusion Services and Education

CAREERS

©2026 Omnicare® a CVS Health Company

Exhibit D

Omniview Privacy Policy

Omnicare | Omniview
a CVSHealth. company

Privacy Policy

Go Back

Effective Date: October 31, 2022

This Privacy Policy describes how Omnicare, Inc., a wholly owned subsidiary of CVS Health ("Omnicare," "we" or "us") may collect information about you through your interactions with us on **https://omniview.omnicare.com** and on our other websites (collectively, the "Omniview Portal"). By using the Omniview Portal, you agree to the terms of this Privacy Policy. If you have any questions or concerns about this Privacy Policy, or about the way your information is collected and used, please call us toll-free at 1-888-607-4287.

We may change this Privacy Policy. The "Effective Date" legend at the top of this page indicates when this Privacy Policy was last revised. Any changes will become effective when we post the revised Privacy Policy on the Omniview Portal. Your use of the Omniview Portal following these changes means that you accept the revised Privacy Policy.

Who May Use the Omniview Portal

We do not knowingly collect personal information online from any person we know to be under the age of 13 and instruct users under 13 not to send us any information to or through the Omniview Portal.

The Omniview Portal is designed for users from, and are controlled and operated by us from, the United States. By using the Omniview Portal, you consent to the transfer of your information to the United States or storage of your information in the United States, which may have different data protection rules than those of your country

The Personal Information We Collect

We want you to understand how personal information you provide to us is collected and used. Personal information is any information that we can use to identify, locate, or contact you. We may collect and store your personal information when you provide it to use or to our service providers. Some examples of personal information we collect and when we collect it include:

- Contact Information: name, facility address, telephone number(s), email address, job title or role.
- If you are a nurse or a facility's agent or member, to allow you to send and receive secure messages to and from Omnicare through the Omniview Portal.

- If you are an Omnicare employee, to allow you to send and receive secure messages to and from other Omniview Portal users.
- To allow you to access and execute required authorization documents, through the Omniview Portal, necessary for (re)ordering prescriptions for the facility and/or the facility's patients; and
- To allow you to track the status of such (re)orders as a convenience to you, your facility, and your patients.

If you choose not to provide your personal information to us, we may not be able to provide you with requested products, services or information.

If you submit any personal information relating to other people in connection with the Omniview Portal, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

We may combine the information collected from you through the Omniview Portal with information we receive from and about you from other online and offline sources and use the combined information in accordance with this Privacy Policy.

Use and Disclosure of Personal Information

We use your personal information to respond to your requests, such as to fulfill your order, contact you with information about your order, send you email alerts, send you newsletters, and to provide you with related customer service. We may also use your information to send marketing communications and administrative information to you, as permitted by law and our client agreements.

We may use personal information to personalize your experience on the Omniview Portal, including by presenting products and content tailored to you, and for our business purposes, such as data analysis, audits, fraud monitoring and prevention, developing the Omniview Portal and new products and services, determining the effectiveness of our promotional campaigns, and operating and expanding our business activities.

In the event that Omnicare or some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security, or to the extent we engage in business negotiations with third parties, personal information may be transferred to or shared with third parties as part of any such transaction or negotiation.

To the extent permitted by applicable law, we may provide personal information to our affiliated businesses or to our business partners, who may use it to send you marketing and other communications.

We may disclose personal information to our service providers, who provide services such as website hosting, data analysis, information technology and related infrastructure provision, customer service, email delivery, auditing, and other services.

If we are requested by law enforcement officials or judicial authorities to provide personal information, we may do so. In matters involving claims of personal or public safety or in litigation where the information is pertinent (including to allow us to pursue available

remedies or limit the damages that we may sustain), we may use or disclose personal information, including without court process. We may also use or disclose personal information to enforce our terms and conditions, to protect our operations or those of any of our affiliates, or to protect our rights, privacy, safety, or property and/or that of our affiliates, you, or others.

We may use and disclose personal information to investigate security breaches or to cooperate with authorities.

We may use and disclose information that does not personally identify you (including the information described under "Cookies and Other Technologies," below) for any purpose, except to the extent limited by applicable law. If we are required to treat such information as personal information under applicable law, then we may use it for all purposes for which we use and disclose personal information.

We may combine information that does not personally identify you with personal information. If we do, we will treat the combined information as personal information as long as it is combined.

Links

The Omniview Portal may contain links to, or otherwise make available, third-party websites, services, or other resources not operated by us or on our behalf ("Third Party Services"). These links are provided as a convenience only and do not constitute an affiliation with, endorsement, or sponsorship of the Third Party Services. Any information you provide to such third parties is not subject to the terms of this Privacy Policy, and we are not responsible for the privacy or security of the information you provide to them or their handling of your information. We recommend that you review the privacy policy of any third party to whom you provide personal information online.

In addition, we are not responsible for the information collection, use, disclosure, or security policies and practices of other organizations, such as Apple, Google, Microsoft, RIM, or any other app developer, app provider, operating system provider, wireless service provider, or device manufacturer.

Information from Other Sources

We may collect data about you from publicly available sources to personalize your experience. We may also obtain data provided by third parties. For example, we may obtain information from companies to improve the accuracy of the information we have about you (e.g., adding your zip code to your address information). This improves our ability to contact you and increases the relevance of our offers and communications to you.

Security

We seek to use reasonable physical, technical, and administrative safeguards to protect personal information within our organization. Unfortunately, no data transmission or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account with us has been compromised), please immediately contact us in accordance with the "Contact Information" section below.

Your identity verification information is provided to the organization you are currently associated with. Your organization is responsible to verify your identity, your access to the Omniview Portal and of your access to your facilities residents' information.

You are responsible for maintaining the confidentiality of your Omniview Portal access information and password and for restricting access to your device, and you agree to accept responsibility for all activities that occur under your password.

Telephone, Text and Fax Policy

By providing your business, residential or wireless phone and/or fax number(s) to Omnicare, you expressly consent to receive marketing and non-marketing autodialed and/or prerecorded calls, text messages and faxes (including fax advertisements) from or on behalf of Omnicare, at the number(s) provided. Your consent to receive calls or texts on your wireless device is not a condition of any purchase. Consent may be revoked at any time by calling the toll-free number at 1-800-SHOPCVS or faxing your opt-out request to 1-401-652-0893. You may also send an opt-out request via email to **do_not_call@cvscaremark.com** with the phone and/or fax number you wish to opt-out. Your wireless carrier's standard message and data rates may apply.

Text Messaging Terms and Conditions

Omnicare or one or more of its affiliates offers access to pharmacy and healthcare service messages via recurring SMS (Short Message Service) and MMS (Multimedia Message Service) text alerts. Enrollment in text alerts requires you to provide your own mobile phone number with an area code within the 50 United States or the District of Columbia. By enrolling to receive Omnicare text alerts, you agree to these terms and conditions, which become effective upon your enrollment. You may be asked to verify your mobile phone number before the service will start. This requires responding to a text alert sent to your mobile phone confirming your enrollment in this Service.

You acknowledge that text alerts will be sent to the mobile phone number you provide to Omnicare. Such alerts may include limited personal information about your prescriptions, and whoever has access to the mobile phone or carrier account will also be able to see this information. Once you enroll, the frequency of text alerts we send to you will vary. You will typically receive text alerts when we have information for you about your prescriptions or other healthcare information. Omnicare does not impose a separate charge for text alerts; however, your mobile carrier's message and data rates may apply depending on the terms and conditions of your mobile phone contract. You are solely responsible for all message and data charges that you incur. Please contact your mobile service provider about such charges. The following carriers are supported: AT&T;, Sprint, Boost, Verizon Wireless, U.S. Cellular®, T-Mobile®, Cincinnati Bell, Alltel, Virgin Mobile USA, Cellular South, Unicel, Centennial and nTelos. You may opt out of Omnicare text alerts at any time. To stop receiving text alerts, call the toll-free number at 1-800-SHOPCVS or faxing your opt-out request to 1-401-652-0893. You may also send an opt-out request via email to **do_not_call@cvscaremark.com** with the phone and/or fax number you wish to opt-out.

The Omnicare text alert programs are offered on an "as is" basis and: (1) may not be available in all areas at all times; and (2) may not continue to work in the event of product, software, coverage or other service changes made by your wireless carrier. Omnicare may change or discontinue any of its text alert programs without notice or liability to you.

Omnicare and its related companies and each of their respective officers, directors and employees are not responsible and shall not be liable for any losses or injuries of any kind resulting, directly or indirectly, from any Omnicare text alert program or from technical failures or delays of any kind. Omnicare reserves the right to cease delivery of text alerts to any person at any time in its sole discretion.

Cookies and Other Technologies

Like many other websites and online services, we collect information about the Omniview Portal's traffic and usage patterns through the use of cookies, Web server logs, web beacons and other, similar technologies. We use this information for various purposes, such as to ensure that the Omniview Portal functions properly, to facilitate navigation, to personalize your experience, to understand use of the Omniview Portal, to diagnose problems, to measure the success of our marketing campaigns and target advertisements, and to otherwise administer the Omniview Portal.

Cookies are small computer files we transfer to your computer's hard drive. These small text files help us personalize content on our pages. Your browser software can be set to reject or accept cookies. Instructions for resetting the browser are available in the Help section of most browsers.

Our use of cookies also allows us to collect and receive certain information about a website user, such as the type of Web browser used by our customer. Reviewing our Web server logs and our customers' use of our site helps us to, among other purposes, statistically monitor how many people are using our site and for what purpose.

Pixel tags are a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is open. Pixel tags are often used in combination with cookies.

Your IP address is a number that is automatically assigned to the computer that you are using by your Internet Service Provider. An IP address may be identified and logged automatically in our Web server log files whenever a user accesses the Omniview Portal, along with the time of the visit and the page(s) that were visited. Collecting IP addresses is standard practice and is done automatically by many websites, applications and other services. We use IP addresses for purposes such as calculating usage levels of the Omniview Portal, helping diagnose server problems, and administering the Omniview Portal.

We may use Adobe Flash Local Stored Objects ("LSOs") and other technologies to, among other things, collect and store information about your use of the Omniview Portal. If you do not want Flash LSOs stored on your computer, you can adjust the settings of your Flash player to block Flash LSO storage using the tools contained in the Website Storage Settings Panel. You can also control Flash LSOs by going to the Global Storage Settings Panel and following the instructions (which may include instructions that explain, for example, how to delete existing Flash LSOs (referred to "information" on the Macromedia site), how to prevent Flash LSOs from being placed on your computer without your being asked, and (for Flash Player 8 and later) how to block Flash LSOs that are not being delivered by the operator of the page you are on at the time). Please note that setting the

Flash Player to restrict or limit acceptance of Flash LSOs may reduce or impede the functionality of some Flash applications.

Tracking/Third-Party Advertisers

We may use or partner third-party companies, including social media companies like Facebook, as well as third-party advertising companies to provide measurements services and display targeted advertisements regarding goods and services that may be of interest to you when you access and use the Services; these targeted advertisements are based on information relating to your access to and use of the Services and of other online services. To do so, these companies may place or recognize a unique cookie on your browser including through the use of pixel tags, web beacons, and other storage technologies to collect or receive information from our website and elsewhere on the internet. We may use analytics providers that use cookies, pixel tags, web beacons, and other, similar technologies to collect or receive information about your use of the Services and your use of other websites or online services.

You may opt out of the collection and use of information for advertisement targeting, at any time. To acquire further information and exercise your right to opt out you may defer to consumer choice tools created under self-regulation programs, such as **http://www.networkadvertising.org/managing/opt_out.asp** and **http://www.aboutads.info/.**

Note: Even if you opt out of targeted advertisements, you may still see or receive other types of online advertising based on factors such as general location derived from your IP address, your browser type, and your search terms.

Lastly, you may manage cookies in your web browser. Your browser software can be set to reject or accept cookies. Instructions for resetting the browser are available in the Help section of most browsers.

We do not respond to browser do-not-track signals.

Fraudulent Sites, Spam & Phishing

Please be aware that there may be fraudulent websites that illegally use Omnicare logos, and other aspects of the Omnicare brand. Omnicare is in no way associated with any fraudulent websites. These sites may circulate their presence on the internet via spam email, or through fraudulent phishing practices.

These sites have not been authorized by Omnicare to use our name and we work aggressively to identify their source and have them shut down. If you are in receipt of this type of spam email, to help protect your privacy you should avoid replying to it or forwarding it to other people.

In addition to our official websites, Omnicare works with a number of third parties that host websites and micro-sites that provide information and services to our customers. If you are concerned that a website or an email may be fraudulent, please contact us by phone at 1-855-LET-OMNI (538-6664) with your concerns.

Your Choices and Access

You can take yourself off our email list for promotional offers at any time by updating your Notification Preferences in your account profile under **Edit My Profile**. If you opt out of receiving promotional emails from us, we may still send you important administrative messages, from which you cannot opt out.

You can request the removal or modification of the personal information you have provided to us by sending an email to the appropriate area under "Contact Us". For your protection, we may only implement requests with respect to the personal information associated with the particular email address that you use to send us your request, and we may need to verify your identity and obtain information on the context in which you provided your personal information before implementing your request. We will try to accommodate your request as soon as reasonably practicable.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting such change or deletion. There may also be residual information that will remain within our databases and other records, which will not be removed.

Your California Privacy Rights

If you are our customer and a California resident, you may request that we provide you with certain information about the entities with which we have shared our customers' personal information for direct marketing purposes during the preceding calendar year. To do so, please write to us at **ConsumerPrivacy@cvshealth.com.**

Deidentified Patient Information

In addition to personal information, we may sell or disclose patient and/or member information that has been deidentified as permitted by law. To the extent we sell or share such deidentified patient and/or member information, we do so pursuant to one of the deidentification methodologies described in Section 164.514(b)(1) or (b)(2) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method and the HIPAA safe harbor method, respectively.

Your Responsibility

By establishing an Omniview Portal account, you agree that it is your responsibility to:

- Authorize, monitor, and control access to and use of your **https://omniview.omnicare.com**, User ID and password.
- Promptly inform us of any need to deactivate a password or an account by calling Customer Service at 1-855-LET-OMNI (538-6664).

Contact Information

If you have any questions or concerns about this statement, or about the way your information is collected and used, please **Contact us** or call us toll-free at 1-855-LET-OMNI (538-6664).

If you have any questions about the content of this Privacy Policy, please contact us at **webadministrator@omnicare.com** or the CVS Health Privacy Office at the following address:

CVS Health
Attn: Privacy Office
One CVS Drive
Woonsocket, R.I. 02895
1-888-607-4287

Go Back

Copyright © 2023 Omnicare, Inc. CONFIDENTIAL INFORMATION 20230413.1

Exhibit E

Workforce Privacy Policy

Workforce Privacy Policy

Effective date: July 3, 2025

This Workforce Privacy Policy talks about how CVS Pharmacy®, Inc. and its subsidiaries and affiliates ("CVS," "we," "us," or “our”) may collect and use personal information about our employees, job applicants, former employees, contractors and other CVS professionals. This Workforce Privacy Policy does not apply to CVS customers, patients or health plan members.

If you have any questions or concerns about this Workforce Privacy Policy, how we collect and use your personal information, or questions about which policy applies to information you have provided, please do not hesitate to contact us, or call us toll-free at **1-888-607-4287**.

We may change this Workforce Privacy Policy. The "effective date” at the top of this page shows when it was last revised. Any changes take effect when we post the revised Workforce Privacy Policy.

If you are a California consumer, for more information about your privacy rights, please see the section of this Workforce Privacy Policy called “Your California privacy rights.”

TABLE OF CONTENTS

1. The personal information we collect
2. Sources we collect personal information from
3. How we use your personal information
4. How we disclose personal information
5. Third-party services and features
6. Security
7. Cookies and other technologies
8. Contact information
9. Your California privacy rights

1. The personal information we collect

We want you to know how we collect and use your personal information. Some examples of the personal information we may collect about you include:

Information from you:

- Contact information including your name, mailing address, personal email address, personal telephone and contact numbers, emergency contacts and language preferences
- Demographic information, such as your age and date of birth, sex and gender, race and ethnicity, sexual orientation and gender identity, disability and health status and military status
- Professional information, such as resumes and cover letters, educational history and transcripts, work history, references, certifications and professional licenses
- Work eligibility and tax information, such as your social security number, spousal and dependent information and marital status

- Vehicle information, such as VIN and license plate number
- ID information, such as driver's license information, passport number, government-issued identification number and immigration/naturalization identification number
- Financial information, such as bank account numbers and beneficiary information
- Social media account information if you share it with us
- Photos or videos you provide to us
- Other information you voluntarily provide

Information created during your workforce relationship with CVS:

- Role information, such as job title, office location, start and end dates, business unit and reporting manager
- Compensation information, such as salary and wages, bonus allocations and payments, hours of work and records of absence
- Benefits information, such as insurance enrollments and 401(k) contributions
- Workforce investigations, grievances and complaints, disciplinary action and performance evaluations
- Background check and investigations information
- Information about your internet activity and related devices, including your computer's IP address and/or mobile device information (e.g., device model, operating system version, unique device identifiers, mobile network information)
- Geolocation information, including from your mobile device(s) or vehicle(s), such as GPS coordinates
- Health information, such as your health conditions
- Images or videos recorded in or around one of our stores or office buildings (e.g., security camera footage)

We may also combine information that does not personally identify you with personal information. If we do, we will treat the combined information as personal information for as long as it stays combined. Please note, we may use and disclose de-identified information that is not in scope of this policy.

2. Sources we collect personal information from

We collect the personal information described above from the following sources.

- **Directly from you.** We collect personal information directly from you when you interact with us or our vendors through communications and automatically when you visit our websites and mobile applications.
- **From subsidiaries and affiliates.** We collect personal information from our subsidiaries and affiliates you interact with as permitted by applicable law.
- **Publicly available information and other sources.** We may collect information about you from both publicly available and other third-party sources to enhance and improve the accuracy of our information about you. We may combine the information we collect from you through the services with information we get from and about you from other online and offline sources. We may use the combined information in accordance with this Workforce Privacy Policy.

3. How we use your personal information

Depending on the nature of your relationship with us, we may use your personal information for the purposes listed below.

- **To communicate with you.** We use your personal information to respond to your requests and otherwise communicate with you. For instance, we may use your personal information to consider you for a role, contact you about your application, send you email alerts, send you newsletters and to provide you with related customer service. We may use your personal information to send marketing communications and administrative information.
- **For our internal business purposes.** We may use your personal information for our internal human resources and business purposes, such as hiring and onboarding, offboarding, financial reporting, training and data analysis. We may also use it for developing our new programs, to assess the effectiveness of our campaigns, and to operate and expand our business activities.
- **For workforce management**. We may use your personal information for payroll and tax, benefits administration, investigations and corrective actions, workforce development programs, diversity, equality and inclusion initiatives.
- **To maintain and enhance the safety and security of the workplace.** We may use personal information to detect, prevent and address safety and security issues, fraud or illegal/malicious activity. We may also use your personal information to protect the health and safety of you and others in our workplace.
- **In connection with a sale or transfer of business assets.** To consider and implement mergers, acquisitions, reorganizations and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions.
- **To protect our legal rights and preventing misuse**. To protect the services and our business operations; to prevent and detect fraud, unauthorized activities and access and other misuse; where we believe necessary to investigate, prevent or take action regarding illegal

activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party or violations of our terms and conditions or this Workforce Privacy Policy.

4. How we disclose personal information

We may disclose personal information with the following parties.

- **Vendors.** We may disclose personal Information we collect to our service providers or agents who perform functions on our behalf. These may include, for example, IT service providers, help desk, payment processors, analytics providers, consultants, auditors and legal counsel.
- **Affiliates and subsidiaries**. We may disclose personal information we collect to our affiliates or subsidiaries.
- **Government or public authorities**. We may disclose personal information to a third party if (a) we believe that disclosure is reasonably necessary to comply with any applicable law, regulation, legal process or governmental request, (b) to enforce our agreements, policies and terms of service, (c) to protect the security or integrity of our services, (d) to protect the property, rights and safety of CVS, our users or the public from harm or illegal activities, (e) to respond to an emergency which we believe in the good faith requires us to disclose information to assist in preventing the death or serious bodily injury of any person, or (f) to investigate and defend ourselves against any third-party claims or allegations.

We may disclose personal information for the following purposes:

- **To provide information to our service providers.** We may disclose personal information to our service providers. They provide services such as website hosting, data analysis, payment processing, order fulfillment, information technology and infrastructure, customer service, email delivery, auditing and other services.
- **In connection with a sale or transfer of business assets.** We may disclose or transfer your personal information to other parties if some or all of our business, assets or stock are sold, transferred or used as security. This includes in connection with any bankruptcy or similar proceeding.
- **To respond to law enforcement officials or enforce our rights.** We may disclose your personal information if required to do so by law enforcement officials or other government authorities. We disclose personal information in matters involving claims of personal or public safety, or in litigation. This may include disclosure of your personal information to allow us to pursue remedies or to limit the damages we may sustain. We may also use or disclose your information to enforce our terms and conditions, to protect our operations or those of any of our affiliates, to prevent misuse of our services, or to protect our rights, privacy, safety or property and/or that of our affiliates, you or others.
- **To maintain and enhance the safety and security of the workplace.** We may disclose personal information to detect, prevent and address safety and security issues, fraud or illegal/malicious activity. We may also disclose your personal information to protect the health and safety of you and others in our workplace.

5. Third-party service and features

The services may contain links to, or make available, third-party websites, services, features or other resources not run by us or on our behalf (the “Third-Party Services.”) We

make these Third-Party Services available as a convenience to you and are not affiliated with, endorsing or sponsoring the Third-Party Services.

Any information you give to such third parties is not subject to the terms of this Workforce Privacy Policy. We are not responsible for the privacy or security of the information you give to Third-Party Services or how they handle your information. We also are not responsible for the information collection, use, sharing or security practices of Third-Party Services. You should review the privacy policy of any Third-Party Service to whom you give information in connection with the services.

6. Security

We use reasonable physical, technical and administrative safeguards. Please be aware that despite our efforts, no data security measures can guarantee security. You should take steps to ensure your personal information is protected like using passwords that would be difficult to guess, not using the same password for multiple accounts and periodically changing your password.

7. Cookies and other technologies

What are cookies? Cookies are small computer files we transfer to your computer's hard drive. These are usually small text files. You can set your browser to accept or reject cookies. Instructions for resetting the browser are in the "help" section of most browsers.

How we use cookies. Like many other websites and online services, we collect traffic and usage patterns. We use cookies, web server logs and similar technologies to do this.

We use this information for various purposes:

- To ensure that the services function properly
- To help with navigation (or how you find your way around the site)
- To understand use of the services
- To diagnose problems
- To measure the success of our talent campaigns
- To otherwise administer the services

We also use cookies to collect and receive certain information about a website user, such as the type of web browser used, internet service provider (“ISP”), referring/exit pages, operating system, date/time stamp, clickstream data, device platform, device version and/or other device characteristics including your choice of settings such as Wi-Fi, Bluetooth and Global Positioning System ("GPS"), CPU ID and type, build, model, manufacturer, operating system version, screen size, screen resolution, mobile network status, device locale and carrier ID. We review our web server logs and usage of our sites. This helps us to gather statistics on how many people are using our sites and why.

Internet providers assign your device an IP address number. We may identify and log your IP address automatically in our web server log files when you use our services. We may also collect the time of your visit and the pages you look at. We use IP addresses to do things like gauge usage levels of the services, help find server problems, and administer services.

Our services use tracking technologies to collect and record your activities and movements across our websites throughout your browsing session, including page hits, mouse movements, scrolling, typing, out-of-the-box errors and events and API calls (“Session Data”). We use this information to (1) remember your information so you do not have to re-enter it, (2) track and understand how you use and interact with the services, (3) perform analytics, (4)

measure the usability of the services and the effectiveness of our communications; and (5) improve our products, services and your experience. Such tracking may also include recorded sessions, which we may play back for these purposes. We may share session data with our vendors (which may change over time) for these purposes.

Do-Not-Track. Our websites are not designed to respond to "do-not-track" signals received from browsers.

8. Contact information

If you have any questions or concerns about the way we collect and use your information, contact us, or call us toll-free at **1-888-607-4287.**

If you have any other questions about the content of this Workforce Privacy Policy contact the CVS Health® Privacy Office at the address below.

CVS Health
Attn: Privacy Office
1 CVS Drive
Woonsocket, R.I. 02895
1-888-607-4287

9. Your California privacy rights

Last Updated: July 3, 2025

This section supplements the Workforce Privacy Policy and applies solely to California employees, job applicants, former employees, contractors and other CVS professionals about whom we have collected personal information from any source, including through the use of our website(s), mobile applications or other online services, or by communicating with us electronically, in paper correspondence or in person (collectively, "you"). Under the California Consumer Privacy Act, as amended

by the California Privacy Rights Act of 2020 (the "CCPA"), California residents have the right to receive certain disclosures regarding our information practices related to "personal information," as defined under the CCPA.

This section does not address or apply to our information practices that are not subject to the CCPA, such as:

- **Publicly available information**. Information that is lawfully made available from government records, information we have a reasonable basis to believe is lawfully made available to the general public by you or by widely distributed media or by a person to whom you have disclosed the information and not restricted it to a specific audience.
- **Deidentified information**. Information that is deidentified in accordance with applicable laws.
- **Aggregated information**. Information relates to a group from which individual identities have been removed.
- **Protected health information**. Information governed by the Health Insurance Portability and Accountability Act or California Confidentiality of Medical Information Act.
- **Activities covered by the Fair Credit Reporting Act**. This includes information we receive from consumer reporting agencies that are subject to the Fair Credit Reporting Act e.g., information contained in background check reports we obtain as part of our vetting process.
- **Trade secret and intellectual property of CVS**. This includes our confidential business information and intellectual property.

The terms used in this section have the same meaning given to them in the CCPA.

A. What personal information we collect

We may collect the following categories of personal information (as enumerated in the CCPA) about you. For more information about the personal information we collect, please see Section 1 above.

- **Identifiers**, which may include your name, mailing address, personal email address, and personal telephone number
- **Professional or employment-related information**, such as your employment history, information relating to your compensation, benefits information, information from background checks or references, information relating to your performance evaluations, hours of work and records of absence and other information that may be provided on your resume
- **Commercial information**, such as VIN or vehicle license plate number
- **Information relating to internet activity or other electronic network activity**, which may include your device and browser information, interactions with our websites or mobile sites, mobile apps, Wi-Fi, emails, communications and social media
- **Geolocation data**, including from your mobile device(s) or vehicle(s), such as Global Positioning System ("GPS") coordinates
- **Audio, electronic or visual information**, which may include images you provide to us (e.g., when you upload photos or videos) or that are viewed or recorded on a security camera
- **Education information**, such as education history, educational degrees and academic transcripts
- **Protected classification characteristics under California or federal law**, such as your age and/or date of birth, gender or gender identity, nationality and national origin, race or ethnicity, marital status, criminal history, drug test results and trade union membership
- **Personal information categories listed in the California Customer Records statute (Cal. Civ. Code §**

1798.80(e)), such as your health insurance information and workers' compensation claim information, signature and physical characteristics or description

We may also collect the following categories of sensitive personal information about you:

- **Government identification,** such as government issued identifications (e.g., SSN)
- **Account log-in information,** which may include your account username and passwords
- **Demographic information**, such as racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership
- **Precise geolocation data**, such as the GPS coordinates of any corporate devices assigned to you
- **Biometric information**, such as your fingerprint or other biometric identifiers
- **Information concerning your health**, such as your health conditions or information made available via connected health devices (e.g., smart watches, health apps)
- **Information concerning sexual orientation**, as part of our employment reporting obligations and diversity, equality and inclusion initiatives

We do not collect, use or disclose sensitive personal information about employees beyond the purposes authorized by the CCPA.

B. How long we retain personal information

We retain your personal information only as long as necessary and in alignment with our data retention schedules. Information may be retained to comply with applicable law, adhere to contractual requirements, in anticipation of litigation or a legal matter or as otherwise

necessary and proportionate to provide you with a product or service.

C. What we do with personal information

We may use your personal information for the purposes described above in Section 3 of our Workforce Privacy Policy and for the following business and commercial purposes specified in the CCPA:

- Performing services, including maintaining or servicing employment related activities, providing customer service, processing or fulfilling requests, verifying your information, processing payments, providing analytics services or providing similar services
- Auditing related to applicant and employment related activities, including, but not limited to, auditing compliance
- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity and prosecuting those responsible for that activity
- Debugging to identify and repair errors that impair existing intended functionality
- Undertaking internal research for technological development and demonstration
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade or enhance the service or device that is owned, manufactured, manufactured for or controlled by us

D. Sources of collected personal information

We may collect personal information about you from these sources:

- Directly from you or your device, including your use of our websites and mobile applications, and your communications with us
- Our subsidiaries and affiliates
- Our service providers, including but not limited to, technology/website hosting providers, analytics providers, and systems administrators/security and fraud investigations providers
- Advertising networks and social media networks
- Government entities, regulators and law enforcement
- Third parties, including companies that collect and sell publicly available information, or business partners that collect information and provide it to us according to their privacy policies and terms of service

E. What personal information we disclose and who we disclose personal information to

The following table describes the categories of personal information we disclose and the categories of third parties to whom we disclose personal information. For more information about how we disclose personal information, please see Section 4 above.

Categories of Personal Information	**Categories of Third Parties**
Identifiers	- Subsidiaries and affiliates - Government entities, regulators and law enforcement
Commercial information	- Government entities, regulators and law enforcement
Information relating to internet activity or other electronic network activity	- Subsidiaries and affiliates - Regulators, government entities and law enforcement
Geolocation data	- Subsidiaries and affiliates

	- Government entities, regulators and law enforcement
Audio, electronic or visual information	- Government entities, regulators and law enforcement
Education information	- Subsidiaries and affiliates - Government entities, regulators and law enforcement
Professional or employment-related information	- Government entities, regulators and law enforcement
Other personal information not listed above and described in California Civil Code § 1798.80(e)	- Subsidiaries and affiliates - Government entities, regulators and law enforcement
Sensitive personal information	- Government entities, regulators and law enforcement
Information not listed above and related to characteristics protected under California or federal law	- Subsidiaries and affiliates - Government entities, regulators and law enforcement

We do not sell or share your personal information to third parties.

We do not knowingly sell the personal information of minors under 16 years of age.

F. Your privacy rights

If you are a California consumer, you have the following rights under the CCPA with respect to your personal information.

- **Right to know/access.** With respect to the personal information we have collected about you, you have the right to request from us (up to twice per year and subject to certain exemptions): (i) categories of personal information about you we have collected; (ii) the sources from which we have collected that personal information; (iii) our business or commercial purposes for collecting, selling, or disclosing that personal information; (iv) the categories of third parties to whom we have disclosed that personal information; and (v) a copy of the specific pieces of your personal information we have collected.
- **Right to delete.** Subject to certain conditions and exceptions, you may have the right to ask us to delete certain personal information we have collected from you. Please note, CVS is not obligated to delete personal information that is: (i) necessary to provide services that you request (such as benefits and compensation) or (2) required to comply with applicable laws.
- **Right to correction.** You may have the right to ask us to correct inaccuracies in the personal information we have collected.
- **Right to non-discrimination.** We will not discriminate against you if you exercise any of these privacy rights.

How to submit a request

Current Employees: If you are a California consumer and a current CVS employee, then you can reach us one of the ways shown below.

- Go to the Colleague Zone via this link: Submit a General Inquiry
  - Complete and submit the request with your information
  - Under Additional details, write-in, “CA Privacy Rights Request” and then describe the nature of your request in the description box.

- Call us at: **1-888-694-7287**
- **Oak Street Health employees** can call 1-888-776-4854 or email privacy@oakstreethealth.com to submit a request

Former Employees: If you are a California consumer and a former CVS employee, then you can reach us one of the ways shown below.

- Password-protected web portal: **Sign in here**
  - Once you have completed login, navigate to and select the “California Privacy Law” link at bottom of the webpage
  - Next, under “Your Privacy Request” click on the “by submitting your request here”
  - Complete the online submission form
- Call us at: **1-888-694-7287**
- **Former Oak Street Health employees** can call 1-888-776-4854 or email privacy@oakstreethealth.com to submit a request

Applicants and others: If you are a California consumer and a CVS applicant, contractor or other CVS professional, then you can reach us one of the ways shown below.

- **Online submission form**
- Call us at: **1-888-694-7287**
- **Oak Street Health applicants and other professionals** can call 1-888-776-4854 or email privacy@oakstreethealth.com to submit a request

You may also give someone else permission to exercise these rights for you. To submit a request as an authorized agent on behalf of a consumer, write us at **ConsumerPrivacy@CVSHealth.com** or call us at 1-888-694-7287. We will need proof showing you have asked someone else to make a request on your behalf, which may include a Power of Attorney form or other signed

document. If we have information on your minor child, you may exercise these rights for them.

Verifying requests

Before we fulfill a request, we must verify your identity and ability to exercise these rights. There are also some exclusions and exceptions that may apply. So that we can verify your identity, if you are a CVS employee or former employee, you will need to first sign into your account. If you are not a CVS employee or former employee, you will be asked to give us certain personal information via webform or on the phone, as described above. If you are not a CVS employee or former employee and request access to, correction or deletion of your personal information, we may require you to provide any of the following information: Full legal name, email address, phone number, position(s) applied for, store/office location applied to and/or home address (depending on the information you may have provided). In addition, if you are not a CVS employee or former employee and you ask us to provide you with specific pieces of personal information, we may require you to sign a declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request.

CCPA reporting metrics

To learn more about the consumer requests that CVS has processed in the past calendar year, click here.