Instructions: These are the Policies and Procedures which are required by the HIPAA Privacy Rules. As the employer, we need to complete it on behalf of our health plan. Note that these Polices and Procedures are, technically, the "plan's" policies and procedures. So, when the Policies and Procedures refer to "us" or "we" the Policies and Procedures are referring to the health plan. This can be confusing, but HIPAA treats the "health plan" as a separate entity, different from the "employer".

loanDepot.com LLC Welfare Benefits Plan

HIPAA PRIVACY POLICIES & PROCEDURES

These HIPAA Privacy Policies and Procedures implement our obligations to protect the privacy of individually identifiable health information that we create, receive or maintain as a group health plan. **loanDepot.com, LLC** (the "Sponsor") is the sponsor of the **loanDepot.com LLC Welfare Benefits Plan** (the "Plan"), to whom these Policies and Procedures apply.

Sponsor adopts these policies, along with the attached forms, on behalf of the Plan. The Plan implements these Health Information Privacy Policies and Procedures as a matter of sound business practice, to protect the interests of our enrollees, and to fulfill our legal obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 ("Privacy Rules"). If we are uncertain of the meaning of a term we will look it up or consult legal counsel.

You are obligated to follow these Health Information Privacy Policies and Procedures faithfully. Failure to do so can result in disciplinary action, including termination of your employment.

If you have questions about any use or disclosure of individually identifiable health information or about your other obligations under these Health Information Privacy Policies and Procedures, the Privacy Rules or other federal or state law, consult our Privacy Official—**Benefits Department**—at **(949) 465-8414** before you act.

Effective Date: **January 1, 2026**

Table of Contents

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

I. USE AND DISCLOSURE POLICIES AND PROCEDURES

Short Summary: HIPAA puts limits on when the plan - and you, as someone who helps the plan - can use or disclose "protected health information." In general, you cannot use or disclose any protected health information unless there is a legally-approved reason to do so. Those reasons are discussed in Sections 1-7. In addition, special rules apply for protected health information related to reproductive health care. See Section 24 for a discussion of those rules. If those rules apply, they supersede the general use and disclosure rules described in this Article I, with respect to such reproductive health care information.

1. Fundamental Policies on Use and Disclosure of Protected Health Information.

Short Summary: There are certain common situations in which you can use or disclose a plan enrollee's protected health information. For example, the plan (or, for example, its third party administrator) can send a $500 check to a hospital and note on the check that the payment was for a particular enrollee's (e.g., "John Smith's") medical expense. This is a disclosure of protected health information but it is for "payment" purposes (discussed further in Section 1(b)(i)).

a) POLICY—No Use or Disclosure. You must not use or disclose protected health information except as these Privacy Policies and Procedures permit or require.

b) Treatment, Payment, Health Care Operations.

i) POLICY—Our Activities. We may use and disclose protected health information, without the individual's permission, for our own payment activities and our own health care operations. As a group health plan, we do not ourselves engage in treatment, though we may be included in the coordination of treatment activities for individuals by health care providers. We may disclose protected health information, without the individual's permission, for any health care provider's treatment activities. We may disclose the minimum necessary protected health information, without the individual's permission, for the payment activities of another covered entity or any health care provider. Special rules apply for disclosures related to another covered entity's health care operations. If this occurs we will consult our legal counsel.

ii) POLICY—Organized Health Care Arrangement's Health Care Operations. When we participate in an organized health care arrangement, we may disclose the minimum necessary protected health information to other covered entity participants in the organized health care arrangement for the health care operations of the organized health care arrangement. This generally allows us to share protected health information with other health plans of our sponsors.

iii) **POLICY—Underwriting and Other Insurance Function Health Care Operations.** We may use and disclose the minimum necessary protected health information for underwriting, premium rating or other activities relating to creation, renewal or replacement of a contract of health insurance or health benefits. We may also use and disclose the minimum necessary protected health information to cede, secure or place a contract for reinsurance of risk for health care claims (including stop-loss and excess loss coverage).

c) **POLICY—Individual or Personal Representative.** We may disclose protected health information to the individual who is the subject of the protected health information and to that individual's personal representative as relevant to the scope of the representation.

d) **POLICY-No Sale, Marketing, Fundraising, Research or Uses of Genetic Information for Underwriting**. We will not directly or indirectly receive remuneration in exchange for any protected health information of an individual, except as otherwise allowed by applicable law. We will not engage in marketing of protected health information, except if such marketing is permissible under HIPAA and does not require an authorization. We will not use or disclose protected health information for fundraising purposes. We will not use or disclose genetic information which is protected health information for underwriting purposes. We will not use or disclose protected health information for research purposes.

e) **POLICY – Special Provisions for Protected Health Information Related to Reproductive Health Care.** We will only use or disclose protected health information which is related to reproductive health care if the additional safeguards described in Section 24 are satisfied. For these purposes, "reproductive health care" means health care that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes.

f) **POLICY - Identify Verification.** We will verify the identity and/or authority of someone prior to making a disclosure, if we are uncertain of either.

g) **PROCEDURE.** Document how you verify the identity and authority of any person, unknown to you, requesting protected health information. Provide the documentation to the Privacy Official, who will retain it for at least six years.

---

2. Informal Permission for Certain Uses and Disclosures.

Short Summary: Be careful about providing a plan enrollee's protected health information to that enrollee's family member of friend. That disclosure is not allowed unless you satisfy an exception (described further in this Section 2).

POLICY—Informal Permission for Certain Uses and Disclosures. We may use with, and disclose to, an individual's family members, other relatives or close personal friends, and any other person that the individual identifies, the individual's minimum necessary

protected health information directly relevant to that person's involvement with the individual's health care or payment related to that health care if we follow all applicable procedures.

PROCEDURE—Individual Present or Not Present. If the individual is present or available and has the capacity to make health care decisions, you must inform the individual of your intent to disclose the protected health information. You may make the use or disclosure if:

- The individual agrees; or
- The individual does not object after a reasonable opportunity to do so; or
- You infer from the situation that, in your professional judgment, the individual does not object.

  If the individual is not present we may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes.

---

3. Authorization for Use or Disclosure.

Short Summary: If you believe you need to make a use or disclosure of protected health information but cannot find any relevant exception, consider asking the plan enrollee to complete an authorization to approve the use of disclosure. This is usually a "safe" choice.

a) POLICY—Authorization. We must have written authorization from the individual (or the individual's personal representative) before we may use or disclose an individual's protected health information for any purpose, except for the following:

- For treatment, payment or health care operations.
- To the individual, the individual's personal representative or HHS.
- As permitted for public interest or benefit activities.
- As permitted with a business associate.
- Incidental to otherwise permitted or required uses and disclosures.
- **FORM – Authorization.** Use FORM 3 – Authorization.

b) POLICY—Authorization Revocation or Expiration. We may not rely on an authorization we know has been revoked or has expired. An individual may revoke an authorization at any time. Revocation of an authorization does not affect actions we may have undertaken in reliance on the authorization before we learned of its revocation.

---

4. Public Interest or Benefit Use and Disclosure.

Short Summary: There are a few unusual situations where the plan (or you, on behalf of the plan) can use and disclose protected health information even though the use or disclosure is not for the Plan's payment or health care operations and even though the health plan enrollee has not signed an authorization. These situations are generally noted in this Section 4. For example, a court may order us to disclose the enrollee's protected health information.

a) POLICY—Public Interest or Benefit Use and Disclosure. We may use or disclose an individual's protected health information for the public health, public interest, public benefit, and law enforcement activities listed in this Section 4, without the individual's permission. However, if the protected health information relates to reproductive health care, we will also comply with Section 24.

Use FORM 7 - Disclosure Log/Minimum Necessary to assist with and document your determination of the minimum necessary use or disclosure and to log each disclosure for accounting.

b) Workers' Compensation. We may disclose the minimum necessary protected health information authorized by and needed to comply with workers' compensation or similar programs established by law that provide benefits for work–related injury or illness without regard to fault.

c) Required by Law. We may use or disclose protected health information as required by law. However, if the protected health information relates to reproductive health care, we will also comply with Section 24.

d) Health Oversight Activities. We may disclose the minimum necessary protected health information to a health oversight agency as needed for legally authorized health oversight activities, such as audits, civil, criminal or administrative actions or proceedings, inspections, licensure, certification, disciplinary actions, and appropriate oversight of the health care system or government benefits programs (e.g., Medicare and Medicaid) for which health information is relevant to beneficiary eligibility or entities subject to government regulatory programs or civil rights laws.

e) Judicial and Administrative Proceedings. We may disclose the minimum necessary protected health information in the course of a judicial or administrative proceeding:

i. **Order.** In response to a court or administrative tribunal order, provided we disclose only the expressly ordered protected health information. However, if the protected health information relates to reproductive health care, we will also comply with Section 24.

ii. **Process.** In response to a subpoena, discovery request or other lawful process not accompanied by court or administrative tribunal order, if we:

- Make a reasonable effort to provide notice to the individual sufficient to permit the individual to object to, or seek a qualified protective order from, a court or administrative tribunal; or

- We receive "satisfactory assurance" that the information seeker has made reasonable efforts either (a) to ensure the individual has notice, or (b) to secure a qualified protective order from the court or administrative tribunal or by party stipulation that limits the parties' use or disclosure to the purpose of the proceeding, and requires return or destruction of the protected health information (including all copies) at end of the proceeding. Ask our Privacy Official if we have sufficient "satisfactory assurance".

---

5. Required Disclosures.

Short Summary: Sometimes we must disclose protected health information -- for example, if the U.S. Department of Health and Human Services ("HHS") is auditing our health plan for HIPAA and HHS requests the protected health information.

a) **POLICY—Required Disclosures to Individual or Personal Representative.** We must disclose all protected health information subject to the right of access or disclosure accounting to an individual (or the individual's personal representative) requesting access or disclosure accounting. See Sections 12-14.

b) **POLICY—Required Disclosures to HHS.** We must disclose protected health information to HHS as required for complaint investigation or compliance enforcement or review.

---

6. Minimum Necessary.

Short Summary: When we use or disclose protected health information, we generally can use or disclose the "bare amount" needed. This is called the "minimum necessary" amount for the use or disclosure.

a) POLICY—Minimum Necessary. We must make reasonable efforts to use, to disclose, and to request of another covered entity, only the minimum necessary protected health information to accomplish the intended purpose. This generally will consist of the protected health information contained in a limited data set, although it can be more if needed to accomplish the intended purpose of such use, disclosure or request. There is no minimum necessary limitation for:

- Disclosure to or a request by a health care provider for treatment.
- Use with and disclosure to an individual (or the individual's personal representative).
- Use and disclosure pursuant to an authorization by an individual (or the individual's personal representative).
- Disclosure to HHS for complaint investigation or compliance enforcement or review.
- Use and disclosure required by law.
- Use and disclosure required for compliance with the HIPAA Administrative Simplification Rules.

b) POLICY—Workforce Use. We must make reasonable efforts to limit access to and use of protected health information by our workforce members to the minimum necessary to perform their duties.

☐ Use FORM 7–Disclosure Log/Minimum Necessary to document your compliance with the minimum necessary limitation. Include the completed Form 7 in the individual's records. Send a copy to our Privacy Official.

7. De–Identified Health Information.

Short Summary: Protected health information which has been "de-identified" (so no plan enrollee can be identified) is no longer protected health information and is not subject to HIPAA or these Policies and Procedures.

POLICY—De–Identified Health Information. We may use and disclose de–identified health information without restriction. We will treat as protected health information any key or other means to re–identify health information that has been de-identified.

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

II. RELATIONSHIP RULES

8. Personal Representatives.

Short Summary: In some situations one person (e.g., a parent) is generally allowed to act on behalf of another person (e.g., a child) and receive that second person's protected health information (e.g., a parent generally can receive a child's protected health information.

a) POLICY—Personal Representative. We must consider a personal representative to be the individual for all purposes under these Privacy Policies and Procedures and the Privacy Rules, unless we conclude that the personal representative may be abusive.

b) POLICY—Personal Representatives of Unemancipated Minors. We will grant a parent, guardian or person acting "in loco parentis" (which generally means the parent is acting on behalf of the child) access to and control over an unemancipated minor's protected health information if, and to the extent, applicable State or other law (including case law) permits or requires us to give the parent, guardian, or person acting in loco parentis access or control. If the law is unclear we will discuss the matter with legal counsel.

c) Personal Representatives of Deceased Individuals.

i. POLICY—Information Protected. We will accord the protected health information of a deceased individual all of the privacy protections of these Privacy Policies and Procedures and the Privacy Rules until at least 50 years after the death of the individual. If the individual is deceased, we may disclose to a family member, or other relative or close family friend who is involved in the care or payment for health care of the individual prior to the individual's death, the protected health information that is relevant to such person's involvement. However, we will not make this disclosure if it is inconsistent with the individual's prior expressed preference and that preference is known to us.

ii. POLICY—Rights of Executors. We will furnish an executor, administrator or other person authorized by applicable law to act for a deceased individual or the deceased individual's estate, the same rights with respect to a deceased individual's protected health information that must be accorded the individual, provided the protected health information is relevant to the scope of the representation.

9. Business Associates.

Short Summary: Our health plan (or the employer on behalf of our plan) may hire third parties who will receive protected health information and use or disclose it on our behalf. Before that occurs, we must make sure that third party has signed a contract in which it agrees to follow HIPAA. This contract is called a "business associate agreement."

a) POLICY—Uses and Disclosures with Business Associates. We will not disclose protected health information to a business associate, or allow a business associate to create or receive protected health information on our behalf, unless our Privacy Official or our legal advisers confirms that the business associate has entered into a compliant written contract with us.

The business associate contract requirement does not apply to our permitted disclosures to:

- A health care provider concerning treatment.
- Our plan sponsor.

FORM–Business Associate Contract. We will use FORM 1 - Business Associate Contract Terms or another business associate agreement we find acceptable. We can verify if an agreement is acceptable by using FORM 2 -- Business Associate Agreement Checklist.

b) POLICY—Business Associate Compliance. If we learn that a business associate has materially breached the business associate contract, we will require the business associate to promptly cure the breach. If the business associate fails to cure the breach to our satisfaction, we will terminate the business associate contract and our business associate relationship with that business associate.

---

10. Plan Sponsors and Third-Party Administrators.

Short Summary: Under HIPAA an employer generally cannot receive protected health information unless it has agreed to follow HIPAA's requirements. There can be a few exceptions, such as "enrollment information". This exception allows the employer to know which employees are in (or out) of the health plan and which level of coverage (e.g., single or family) those employees have selected.

a) POLICY—Disclosure of Protected Health Information to Plan Sponsors. We may not disclose, and we may not permit a health insurance issuer, HMO, third party administrator, or other business associate to disclose on our behalf, protected health information to our plan sponsor—the employer, union or other entity that established and maintains our group health plan—unless we have the authorization or other sufficient permission of each plan participant and beneficiary whose protected health information is to be disclosed. There are three exceptions:

i. Enrollment Data to Plan Sponsor. Our plan sponsor may receive from us, and from a health insurance issuer, HMO, third party administrator, or other business associate on our behalf, the minimum necessary information to determine whether an individual is or is not participating in our group health plan.

ii. Summary Health Information to Plan Sponsor. Our plan sponsor may receive from us, and from a health insurance issuer, HMO, third party administrator, or other business associate on our behalf, the minimum necessary summary health information to enable our plan sponsor to either (a) obtain premium bids for providing coverage under our group health plan, or (b) modify, amend or terminate our group health plan. However, notwithstanding the prior sentence, we may not disclose genetic information which is protected health information as part of this summary health information provision.

iii. Plan Administration Functions by Plan Sponsor. Our plan sponsor may receive from us, and from a health insurance issuer, HMO, third party administrator, or other business associate on our behalf, the minimum necessary protected health information of our plan participants and their beneficiaries to enable our plan sponsor to perform plan administration functions for us, provided that our plan sponsor furnishes written certification that the group health plan document has been amended to include “satisfactory assurance” that our plan sponsor will appropriately safeguard and limit use and disclosure of the protected health information, including not using or disclosing the protected health information for any employment-related action or decision or in connection with any other benefit or benefit plan.

FORM 3–Plan Sponsor's Group Health Plan Document Amendment contains the mandatory terms for our plan document that the Privacy Rules require to evidence the plan sponsor’s “satisfactory assurance.”

FORM 4–Plan Sponsor’s Certification of Group Health Plan Document Amendment is an example of the certification of “satisfactory assurance” our plan sponsor must make.

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

III. INDIVIDUAL'S INFORMATION RIGHTS

11. Privacy Practices Notice.

Short Summary: Our health plan is required under HIPAA to send a notice to plan participants explaining their privacy rights under HIPAA. We must send out that notice to new participants (or arrange to have another entity send it, such as our third party administrator) and then periodically send out reminders about the notice.

a) POLICY—Privacy Practices Notice. As a self-funded group health plan, we will maintain a Privacy Practices Notice. That Notice must give individuals written notice of the uses and disclosures of protected health information that we may make, our legal duties with respect to protected health information, and individuals' privacy rights and how to exercise them. We must use and disclose protected health information consistently with our Notice. Use FORM 7 – Privacy Practices Notice as a template for our Privacy Practices Notice.

b) POLICY—Revision to Privacy Practices Notice. We will promptly revise our Privacy Practices Notice whenever there is a material change to our uses or disclosures of protected health information, to our legal duties, to the individuals' rights or to other privacy practices that render the statements in our Notice no longer accurate.

PROCEDURE—Privacy Practices Notice Distribution. Our Privacy Official will distribute (or cause to be distributed) the appropriate Privacy Practices Notice to each individual who is our plan participant. If there is a change to the Privacy Practices Notice and we maintain a web site, we may (in lieu of distributing the revised Notice in paper form) prominently post the change or the revised Notice on our web site. If we do this, we will post the Notice or change by the effective date of the material change. We will also provide the revised Notice, or information about the material change and how to obtain the revised Notice, in our next annual mailing to individuals then covered by the plan. We will also:

- Disseminate our Notice to each new plan participant at enrollment.
- Notify our then current plan participants, at least once every 3 years, that our Notice is available on request, explaining how the participants may obtain it.
- Ensure that our Notice is prominently posted and electronically available on each web site the health plan maintains (if any) that provides information about our benefits.
- Disseminate any revised Notice to our then current plan participants within 60 days of the material change. We will not implement the material change in our privacy practices before the effective date of our revised Notice (unless earlier implementation is required by law).

- Furnish our Notice to any person on request.
- Email our Notice to any individual who has agreed to electronic notification and not withdrawn that agreement. We must provide a paper copy of our Notice to the individual, if you know the individual failed to get the email transmission of our Notice or if the individual requests a paper copy.

---

12. Access.

Short Summary: Plan enrollees generally have the legal right to access their protected health information and obtain copies of it. Some new HIPAA rules from 2013 also allow the person to obtain an electronic copy of their protected health information in some situations.

a) POLICY–Right to Inspect and Copy. We will allow an individual to inspect and to obtain a copy of his or her protected health information for as long as we or our business associates maintain that protected health information in designated record sets. We may withhold from an individual only that protected health information specified in Section 12(b) below. We may charge a fee as allowed by law. We generally must respond to the individual's request for access within 30 days of us receiving the request.

If an individual makes an access request with respect to protected health information which is maintained electronically in our designated record set, the following rules shall apply:

- The individual shall have a right to obtain a copy of such information electronically and, if the individual requests, to provide it in the form and format requested by the individual, if it is readily producible in such form and format. If it is not so readily producible, we will provide it in a readable electronic form and format as agreed to by us and the individual.
- The individual shall have a right to direct us to transmit the copy of protected health information directly to another person designated by the individual. We will follow such a direction if the individual's request is in writing, signed by the individual and clearly identifies the designated person and where to send the copy of protected health information.
- Any fee that we may impose for providing the individual a copy of such information shall not be greater than our direct or indirect labor costs, supply costs or postage costs in responding to the request for the copy or for an explanatory summary of the protected health information.
- We will send the information to an individual in an unencrypted email only if we warn the individual of the risks of unencrypted emails and the individual prefers the unencrypted email. We will provide the information on the individual's own external portable media only if we perform a risk analysis related to the potential use of the media and we conclude that there is an acceptable level of risk.

b) POLICY—Protected Health Information We May Withhold. We may deny access to, and a copy of, protected health information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding. Other exceptions may also apply. We will consult our legal counsel if needed.

c) POLICY—Designations. We must identify in writing each designated record set we maintain or that is maintained on our behalf by our business associates, and the titles of persons or offices responsible for receiving and processing access requests. Use FORM 9 – Designated Personnel and Record Sets to identify our designated record sets.

---

13. Amendment.

Short Summary: Plan enrollees generally have the legal right to modify their protected health information that we (or our business associates) hold, if that protected health information is incorrect. We must promptly respond to such a request.

a) POLICY—Right to Amend. We will allow an individual to request to amend his or her protected health information for as long as we or our business associates maintain the protected health information in designated record sets. We may deny an amendment request only as specified in Section 13(b) below. We will generally respond to the individual's request within 60 days of its receipt. If we make an amendment, we will notify our business associates that may have and rely on the unamended records.

b) POLICY—Bases for Denying Amendment Request. We may decline to amend protected health information if:

- We did not create the information (unless the originator is no longer available to act on the request).
- The information to be amended is not part of a designated record set maintained by us or by a business associate on our behalf.
- The information is accurate and complete.

---

14. Disclosure Accounting.

Short Summary: Plan enrollees generally have the legal right to understand how their protected health information has been disclosed. However, as a practical matter the vast majority of the disclosures do not need to be tracked by us or our business associates.

a) **POLICY—Right to Disclosure Accounting.** We will allow an individual to request an accounting of each disclosure that we make of the individual's protected health information for up to 6 years prior to the request. We do not have to account for disclosures that are exempt from accounting as specified in Section 14(b) below. We will respond to the individual's request within 60 days. However, we will not provide a disclosure accounting if a law enforcement official asks us to temporarily not provide it.

☐ We may not charge for an individual's first accounting in any 12-month period. We may charge a reasonable, cost–based fee for other accountings within that same 12-month period.

☐ Use FORM 7 – Disclosure Log/Minimum Necessary to document each accountable disclosure.

☐ The best way to respond to this request is to gather all the required disclosure accounting information from our records and from our business associates' records, then provide all this information to the individual. Alternatively, we may also be able to provide all of the disclosure accounting information we hold, then provide a list of all our business associates, including contact information for those business associates (such as work address, phone number and e-mail address). Before we do this, we would need to ensure the business associate has agreed to directly respond to the individual's request.

b) **POLICY—Exempt Disclosures.** We do not have to account for the following:

- Disclosures made before our Privacy Rules compliance date (generally April 14, 2003 or April 14, 2004). Disclosure relating to an electronic designated record set generally all must be accounted for as of the date specified by HHS.
- Disclosures made to the individual or the individual's personal representative.
- Disclosures made for a payment related to that person's health care, or for health care operations**.**
- Disclosures made pursuant to authorization.
- Disclosures made in a limited data set.

c) **POLICY—Accounting Information.** We will track accountable disclosures. The information that must be tracked to fulfill our disclosure accounting obligations is as follows:

- The disclosure date;
- The name and, if known, address of each person or entity that received the disclosure;
- A description of the protected health information disclosed; and
- A statement of the purpose of the disclosure, or a copy of any written request for the disclosure from HHS or another government agency or organization to which the protected health information was disclosed pursuant to a public interest or benefit activity.

  We will hold this information for 6 years.

---

15. Restriction Requests.

Short Summary: Plan enrollees generally have the legal right to request that we put restrictions on how their protected health information is used or disclosed. Except in very rare situations, we do not have to agree to this request (that is, we can usually deny the request). If we accept the request, we should inform our business associates of the new restriction.

a) POLICY—Restriction Requests. We will allow an individual to request that we restrict our use or disclosure of his or her protected health information for treatment, payment, health care operations, or with specified family members or others. Except as noted below, we have no obligation to agree to such request. We will comply, and notify our business associates to comply, with any such agreement we make (except in an appropriate medical emergency). We will document any agreed-upon restriction request.

We will comply with a restriction request, and notify our business associates to comply, if:

i. the disclosure is to a health plan for purposes of carrying out payment or health care operations and is not otherwise required by law; and

ii. the protected health information pertains solely to a health care item or service for which the individual or another person (other than a health plan on behalf of the individual) has paid the covered entity in full.

b) POLICY—Restriction Termination. We may terminate a restriction agreement (other than a restriction agreement described in the prior sentence) either (i) with the concurrence of the individual or (ii) unilaterally by written notice of termination to the individual. When we terminate a restriction agreement unilaterally, we will continue to comply with the restriction with respect to protected health information we created or received subject to the restriction.

---

16. Confidential Communication.

Short Summary: Sometimes, plan enrollees may be in physical danger if we disclose protected health information in a certain way. For example, suppose our health plan wants to send an explanation of benefits ("EOB") to an employee's home. Suppose the EOB contains sensitive information that an employee is trying to keep from the employee's spouse. The employee may inform us that the employee fears for his / her physical safety if the spouse finds out the employee is being treated for a particular condition (and the EOB would reveal this). So, the employee requests that we (or our third party administrator) send the EOB to the employee's work. We generally must accommodate this type of request.

POLICY—Confidential Communication. We will allow an individual to request confidential communications (that is, the use of alternative means or alternative locations when we communicate protected health information to the individual), if the request is reasonable and in writing, and the individual gives us a clear statement that all or part of the protected health information could endanger the individual if not communicated by the requested alternative means or to the requested alternative location.

IV. ADMINISTRATIVE REQUIREMENTS

17. Privacy Policies and Procedures.

Short Summary: Under HIPAA, our health plan must adopt these policies and procedures. You, as someone who works for the health plan (even if you are employed by the employer) must follow these policies and procedures.

a) **POLICY—Adoption.** We will adopt and implement written privacy policies and procedures for protected health information designed to comply with our obligations under the Privacy Rules. These Privacy Policies and Procedures are intended to satisfy this obligation.

PROCEDURE—Implementation and Compliance. Each member of our workforce with access to protected health information must, at all times, comply with the policies and follow the procedures set out in these Privacy Policies and Procedures.

b) **POLICY—Revisions.** Only a designated person (e.g., plan administrator, plan fiduciary, Privacy Official, etc.) may change these Privacy Policies and Procedures.

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

18. Privacy Personnel, Training, Workforce Management, Administrative Practices.

Short Summary: There are certain administrative practices we must follow. For example, new employees who begin helping out with the plan and who will see protected health information must be trained on HIPAA. In addition, if an improper use or disclosure of protected health information occurs, we must take actions to minimize the harmful effect of that improper use or disclosure.

a) POLICY—Privacy Personnel.

i. Privacy Official. Our Privacy Official is responsible for developing, maintaining, and implementing these Privacy Policies and Procedures, and for overseeing our full compliance with these Privacy Policies and Procedures, the Privacy Rules, and other applicable federal and state privacy law.

Our Privacy Official is Benefits Department, Irvine, CA

Telephone: (949) 465-8414 Fax: (949) 575-5349

E–mail: liveWell@loandepot.com

Office: Irvine, CA

ii. Contact Offices. We will maintain contact offices for individuals to obtain our Privacy Practices Notice and other information on our privacy practices. Our contact offices will also accept complaints about our privacy practices.

Our contact offices are:

Benefits Department, Irvine, CA

b) POLICY—Workforce Training. Each member of our workforce who may have access to or use of protected health information will receive training on our Privacy Policies and Procedures, as necessary and appropriate for the member to carry out his or her job functions. Use FORM 8 – Privacy Training Certificate to document each workforce member's completion of privacy training.

PROCEDURE—Training Timing.

i. New Members. New members of our workforce must receive privacy training before they may have access to or use of protected health information.

ii. **Retraining.** Existing workforce members must receive retraining within a reasonable period of time after there is material change in their job functions or in our Privacy Policies and Procedures that affects their access to or use of protected health information. We may also require periodic retraining even if there has not been any such change.

c) **POLICY—Workforce Sanctions.** Workforce members who violate our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law will be subject to disciplinary action, including employment termination, consistent with the sanctions developed, documented, and disseminated by our Privacy Official and the employer.

d) **POLICY—Mitigation.** We will have and implement contingency plans to mitigate any deleterious effect of an improper use or disclosure of protected health information by a member of our workforce or by our business associates.

e) **POLICY—Retaliatory Acts.** We will not attempt to intimidate, threaten, coerce, discriminate or retaliate against an individual who:

- Exercises any right, including filing complaints, under the Privacy Rules.
- Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by HHS or other appropriate authority.
- Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rules (provided the opposition is reasonable and does not involve illegal disclosure of protected health information).

f) **POLICY—Waivers.** We will not require an individual to waive any right under the Privacy Rules, including the right to complain to HHS, as a condition of providing claims payment, enrollment or benefits eligibility to the individual.

g) **POLICY—Documentation and Record Retention.** We will retain the documentation required by our Privacy Policies and Procedures and the Privacy Rules until 6 years after the later of its creation or last effective date. Our Privacy Official will be our repository of documentation regarding our privacy practices and compliance with our Privacy Policies and Procedures and the Privacy Rules.

---

19. Data Safeguards.

Short Summary: We must ensure that protected health information is kept secure. For example, any protected health information on paper generally should be kept locked up at night.

POLICY—Data Privacy Protection. We will implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of protected health information against any intentional or unintentional use or disclosure in violation of these Privacy Policies and Procedures or the Privacy Rules. These safeguards will include reasonable limits to incidental uses or disclosures of protected health information made as a result of otherwise permitted or required uses or disclosures.

PROCEDURE—Data Privacy Protection. Our Privacy Official, in conjunction with our legal advisers, will augment these Privacy Policies and Procedures with such additional data security policies and procedures as appropriate for our plan to have reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity and confidentiality of the protected health information we maintain against any reasonably anticipated unauthorized use or disclosure, intentional or unintentional, or any reasonably anticipated threat or hazard to the privacy, security or integrity of the protected health information. These additional data security policies and procedures will ensure compliance by our workforce members with these Privacy Policies and Procedures, the Privacy Rules, and such other policies and procedures as may be adopted to implement our compliance obligations under the Privacy Rules.

20. Complaints and HHS Enforcement.

Short Summary: Plan enrollees have the legal right to complain if we are not following HIPAA. We must take those complaints seriously and try to resolve them. In addition, the federal government (usually the Office for Civil Rights, a division of the U.S. Department of Health and Human Services) may audit the health plan to verify that we are following HIPAA.

a) **POLICY—Complaints.** We will timely investigate and appropriately respond to each complaint received by our contact offices or a workforce member regarding our compliance with these Privacy Policies and Procedures or the Privacy Rules.

b) **POLICY—HHS Enforcement and Compliance Cooperation.** We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our plan.

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

V. STATE LAW POLICIES AND PROCEDURES

21. State Privacy Law.

Short Summary: In some situations state privacy laws may go beyond what HIPAA requires. We should carefully consider whether we need to follow those additional requirements. We may take the position that other laws (such as ERISA, a federal law governing many health plans) supersedes those state laws, so that we do not need to follow the state laws. If we do need to follow them, it would be a good idea to modify these Policies and Procedures to reflect those state laws.

POLICY—State Law Compliance. We will comply with state privacy laws to the extent we are required to do so. If our group health plan is subject to ERISA, certain state privacy laws may be preempted. Our Privacy Official and legal advisers will determine which state privacy laws apply to our group health plan, whether those laws conflict with the Privacy Rules and, if so, whether those laws are more stringent than the Privacy Rules and therefore are not preempted by the Privacy Rules.

A state law is more stringent than the Privacy Rules if it provides greater protections or rights to individuals or imposes greater restrictions on our use or disclosure of protected health information than the Privacy Rules.

VI. BREACH RULES

22. Identifying a Breach.

Short Summary: Sometimes we (or a business associate) may experience a "breach" of protected health information (e.g., a former employee takes protected health information with him or her and misuses it). You must promptly report any such breach to the Privacy Official so we can act quickly.

POLICY – Identifying a Breach. We will identify any suspected breach of protected health information and report a suspected breach to our Privacy Official.

FORM – Breach Identification. We will use FORM 10, Breach Identification, to identify a breach. We will record all individuals affected by a breach. We will record the list electronically or by using FORM 11, Log of Individuals Affected by Breach.

---

23. Notification Regarding Breach.

Short Summary: If there was a "breach" of protected health information (as discussed in Section 22), the health plan generally must notify the plan enrollees who were affected. The plan

(generally, us, on behalf of the plan) must inform the U.S. Department of Health and Human Services of the breach.

POLICY – Notification Regarding Breach. We will notify all relevant parties of a breach of protected health information, in accordance with HIPAA's rules. Relevant parties include the U.S. Department of Health and Human Services, affected individuals and, for certain large breaches affecting 500 or more individuals, local media.

FORM - Breach Notification. We will use FORM 10 – Breach Identification and FORM 12 – Notification to Affected Individuals of Breach when notifying relevant parties. We will create a separate notice to the media if so required. If a law enforcement official requests that we delay notice of a breach, we will document our consideration and, where applicable, acceptance of such delay.

24. Special Rules for Protected Health Information Related to Reproductive Health Care.

Short Summary: In April 2024, new regulations imposed additional restrictions on our ability to use or disclose protected health information which is related to reproductive health care ("RHC PHI"). You must follow these special rules when you use or disclose RHC PHI.

a) POLICY— RHC PHI, in General. We, and our business associates, will follow the HIPAA rules related to RHC PHI. This means that we, and our business associates, may not use or disclose RHC PHI for any of the following activities:

i. To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care (all as determined under 45 CFR Section 164.502);

ii. To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care; and / or

iii. To identify any person described in (i) or (ii).

This restriction applies only where the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and we or our business associate that received the request for RHC PHI has reasonably determined that one or more of the following conditions exists:

y. The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided; and / or

z. The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.

In making the determinations in (y) and (z), reproductive health care provided by another person is presumed lawful unless we or our business associate has:

[1] Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided; and / or

[2] Factual information supplied by the person requesting the use or disclosure of protected health information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

b) POLICY – RHC PHI in Specific Situations. We may not use or disclose RHC PHI for purposes related to health oversight activities (as described in 45 CFR Section 164.512(d)), judicial or administrative proceedings (as described in 45 CFR Section 164.512(e)), law enforcement purposes (as described in 45 CFR Section 164.512(f)) or for disclosures to coroners or medical examiners (as described in 45 CFR Section 164.512(g)(1)) without obtaining an attestation that is valid from the person requesting the use or disclosure. We will use our model RHC PHI Attestation for these purposes (FORM 15 – Reproductive Health Care Attestation). If we cannot use FORM 15, our Privacy Official will review the proposed attestation to ensure that it is valid and in compliance with HIPAA and any other applicable law.

In determining the validity of such an attestation, our Privacy Official will verify that the attestation satisfies the requirements of 45 CFR Section 164.509(b)(1) and is not "defective". To satisfy the requirements of 45 CFR Section 164.509(b)(1), the attestation must be for a use or disclosure which is not described in (a)(i), (ii) or (iii) above.

The attestation will be "defective" if it has any of the following defects:

i. The attestation lacks an element or statement required below, in the "Required Attestation Elements" section;

ii. The attestation contains an element or statement not required by 45 CFR Section 164.509(c);

iii. The attestation is combined with any other document except as allowed in 45 CFR Section 164.509(b)(3);

iv. We or our business associate has actual knowledge that material information in the attestation is false; and / or

v. If we or a reasonable covered entity or business associate in the same position would not believe that the attestation is true with respect to a statement that the use or disclosure is not for a purpose prohibited by 45 CFR Section 164.502(a)(5)(iii).

In order for the attestation to be valid, it must contain the following elements:

t. A description of the information requested that identifies the information in a specific fashion, including one of the following: (A) the name of any individual(s) whose protected health information is sought, if practicable; (B) if including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose protected health information is sought;

u. The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure;

v. The name or other specific identification of the person(s), or class of persons, to whom we are to make the requested use or disclosure;

w. A clear statement that the use or disclosure is not for a purpose prohibited under 45 CFR Section 164.502(a)(5)(iii);

x. A statement that a person may be subject to criminal penalties pursuant to 42 USC Section 1320d-6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person;

y. A signature of the person requesting the protected health information (such signature may be electronic) and date. If the attestation is signed by a representative of the person requesting the information, the attestation must provide a description of such representative's authority to act for the person; and

z. The attestation must be written in plain language. It is possible that, in the course of using or disclosing RHC PHI, we were reasonably relying on a facially valid attestation and then we discover information that reasonably shows that the representation made in the attestation was false and prohibited under 45 CFR Section 164.502(a)(5)(iii). In that situation, we must cease such use or disclosure.

52489318v3

BUSINESS ASSOCIATE AGREEMENT

Purpose: A business associate is someone who 1.) Performs functions on behalf of a covered entity (group health plan) or provides services for a covered entity; and 2.) Has access to PHI. Under the 2013 final regulations, the HIPAA privacy and security rules require a business associate agreement to be in place if the business associate has access to PHI.

This Agreement ("Agreement") is effective upon execution by and between loanDepot.com, LLC ("Business Associate") and Anthem ("Health Plan").

Health Plan and Business Associate mutually agree to comply with the requirements of the implementing regulations at 45 Code of Federal Regulations ("C.F.R.") Parts 160-64 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This Agreement shall supersede any prior business associate agreement.

1. Privacy and Security of Protected Health Information.

a) Permitted Uses and Disclosures. Business Associate is permitted to use and disclose Protected Health Information that it creates or receives on Health Plan's behalf or receives from Health Plan (or another business associate of Health Plan) and to request Protected Health Information on Health Plan's behalf (collectively, "Health Plan's Protected Health Information") only:

i) Functions and Activities on Health Plan's Behalf. Except as otherwise limited in this Agreement, to perform functions, activities, or services for, or on behalf of Health Plan as such services may be specified in any underlying agreement(s), provided that such use or disclosure would not violate 45 C.F.R. Part 164, Subpart E "Privacy of Individually Identifiable Health Information" (the "Privacy Rule") or 45 C.F.R. Part 164, Subpart C "Security Standards for the Protection of Electronic Protected Health Information" (the "Security Rule") if done by Health Plan.

ii) Business Associate's Operations. For Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provided that, with respect to disclosure of Health Plan's Protected Health Information, either:

A) The disclosure is Required by Law; or

B) Business Associate obtains reasonable assurance from any person or entity to which Business Associate will disclose Health Plan's Protected Health Information that the person or entity will:

1) Hold Health Plan's Protected Health Information in confidence and use or further disclose Health Plan's Protected Health Information only for the purpose for which Business Associate disclosed Health Plan's Protected Health Information to the person or entity or as Required by Law; and

2) Promptly notify Business Associate (who will in turn notify Health Plan in accordance with Section 4(a)) of any instance of which the person or entity becomes aware in which the confidentiality of Health Plan's Protected Health Information was Breached.

iii) Minimum Necessary. Business Associate will, in its performance of the functions, activities, services, and operations specified in Section 1(a), make reasonable efforts to use, to disclose, and to request only the minimum amount of Health Plan's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum necessary limitation if neither Business Associate nor Health Plan is required to limit the use, disclosure or request to the minimum necessary. Business Associate and Health Plan acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the American Recovery and Reinvestment Act and government guidance on the definition.

b) Prohibition on Unauthorized Use or Disclosure. Business Associate will neither use nor disclose Health Plan's Protected Health Information, except as permitted or required by this Agreement or in writing by Health Plan or as Required by Law. This Agreement does not authorize Business Associate to use or disclose Health Plan's Protected Health Information in a manner that will violate the Privacy Rule or the Security Rule if done by Health Plan, except as set forth in Section 1(a)(ii).

c) Information Safeguards.

i) Privacy of Health Plan's Protected Health Information. Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of Health Plan's Protected Health Information. The safeguards must reasonably protect Health Plan's Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement.

ii) Security of Health Plan's Electronic Protected Health Information. Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Health Plan's behalf as required by the Security Rule, 45 C.F.R. Part 164, Subpart C. Such safeguards will include, but not be limited to, Business Associate conducting periodic risk assessments with respect to Health Plan's Electronic Protected Health Information. Business Associate shall, to the extent reasonably possible, implement and follow recognized security practices consistent with H.R. 7898, enacted into law on January 5, 2021. Business Associate shall provide Health Plan with all information reasonably requested about such safeguards, including whether Business Associate follows such recognized security practices and, if so, which practice or practices.

d) Subcontractors and Agents. Business Associate will require any of its subcontractors and agents, to which Business Associate is permitted by this Agreement or in writing by Health Plan to disclose Health Plan's Protected Health Information and / or Electronic Protected Health Information, to agree to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information, including but not limited to compliance with the applicable requirements of 45 C.F.R. Parts 160, 162 and 164. Such agreement between Business Associate and the subcontractor or agent must be made in writing and must comply with the terms of this Agreement and the requirements outlined at 45 C.F.R. §§ 164.504(e) and 164.314. To the extent required by applicable law or other binding regulatory guidance, Business

Associate shall not disclose Health Plan's Protected Health Information to a "tracking technology vendor" (as defined in guidance issued by the United States Department of Health and Human Services ("DHHS")) unless: (i) Business Associate has entered into an agreement with such tracking technology vendor in accordance with this Section 1(d); and (ii) such disclosure is permitted or required under the Privacy Rule and this Agreement.

e) Prohibition on Certain Activities. Business Associate shall not: (i) sell Protected Health Information (within the meaning of 45 C.F.R. § 164.508); (ii) use or disclose Protected Health Information for fundraising purposes (within the meaning of 45 C.F.R.§ 164.514); (iii) use or disclose Protected Health Information for research (within the meaning of 45 C.F.R.§ 164.512); (iv) use genetic information for underwriting purposes (within the meaning of 45 C.F.R.§ 164.514); or (v) use or disclose Protected Health Information for marketing purposes (within the meaning of 45 C.F.R.§ 164.508). Business Associate shall not de-identify Health Plan's Protected Health Information except if required to perform activities on behalf of Health Plan, as specified in Section 1(a)(i) of this Agreement.

f) Reproductive Health Information. Business Associate shall comply with all requirements imposed on business associates under the HIPAA Privacy Rule to Support Reproductive Health Care Privacy promulgated by DHHS, including, but not limited to, the attestation requirement under 45 C.F.R. § 164.509.

g) Substance Use Disorder Information. The parties acknowledge and agree that records subject to 42 C.F.R. Part 2 ("Part 2") may be used and disclosed only as permitted under Part 2.

2. Compliance with Transaction Standards. If Business Associate conducts in whole or part electronic Transactions on behalf of Health Plan for which DHHS has established Standards, Business Associate will comply, and will require any subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Transaction Rule, 45 C.F.R. Part 162 and any related operating rules. Business Associate shall comply with the National Provider Identifier requirements, if and to the extent applicable. Business Associate shall provide to Health Plan any documentation of compliance with the Transaction Rule which Health Plan may reasonably need, if any, pursuant to section 1104(b) of the Patient Protection and Affordable Care Act, as amended. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any Trading Partner Agreement in connection with the conduct of Standard Transactions on behalf of Health Plan that:

a) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

b) Adds any data element or segment to the maximum defined data set;

c) Uses any code or data element that is marked “not used” in the Standard Transaction’s implementation specification or is not in the Standard Transaction’s implementation specification; or

d) Changes the meaning or intent of the Standard Transaction’s implementation specification.

3. Individual Rights.

a) Access. Business Associate will, within 29 calendar days following Health Plan’s request, make available to Health Plan or, at Health Plan’s direction, to an individual (or the individual’s personal representative) for inspection and obtaining copies Health Plan’s Protected Health Information about the individual that is in Business Associate’s custody or control, so that Health Plan may meet its access obligations under 45 C.F.R. § 164.524.

Effective as of September 23, 2013 and thereafter, if the Protected Health Information is held electronically in a designated record set, then the individual shall have a right to obtain from Business Associate a copy of such information in the electronic form and format requested by the individual, if it is readily producible in such form and format. If it is not so readily producible, Business Associate will provide it in a readable electronic form and format as reasonably requested by Health Plan or, if Business Associate is dealing directly with the individual, the individual. Business Associate shall provide such a copy to Health Plan or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously and specifically made by the individual or Health Plan. In addition, if the individual's request for access directs that the Protected Health Information be transmitted directly to another person designated by the individual, Business Associate must provide the copy to the person designated by the individual, provided the individual's request: (i) is in writing; (ii) is signed by the individual; and (iii) clearly identifies the designated person and where to send the copy of Protected Health Information. If Business Associate provides such a copy to that designated person, Business Associate will promptly notify Health Plan of this fact.

b) Amendment. Business Associate will, within 59 calendar days following notice from Health Plan, amend or permit Health Plan access to amend any portion of Health Plan's Protected Health Information, so that Health Plan may meet its amendment obligations under 45 C.F.R. § 164.526.

c) Disclosure Accounting. So that Health Plan may meet its disclosure accounting obligations under 45 C.F.R. § 164.528:

i) Disclosures Subject to Accounting. Business Associate will record the information specified in Section 3(c)(iii) below ("Disclosure Information") for each disclosure of Health Plan's Protected Health Information, not excepted from disclosure accounting as specified in Section 3(c)(ii) below, that Business Associate makes to Health Plan or to a third party.

ii) Disclosures Not Subject to Accounting. Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of Health Plan's Protected Health Information if Health Plan need not account for such disclosures.

iii) Disclosure Information. With respect to any disclosure by Business Associate of Health Plan's Protected Health Information that is not excepted from disclosure accounting by Section 3(c)(ii) above, Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:

A) Disclosure Information Generally. Except for repetitive disclosures of Health Plan's Protected Health Information as specified in Section 3(c)(iii)(B) below, the Disclosure Information that Business Associate must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) address of the entity to which Business Associate made the disclosure, (iii) a brief description of Health Plan's Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.

B) Disclosure Information for Multiple Disclosures. For multiple disclosures of Health Plan's Protected Health Information that Business Associate makes for a single purpose to the same person or entity (including Health Plan), the Disclosure Information that Business Associate must record is either the Disclosure Information specified in Section

3(c)(iii)(A) above for each accountable disclosure, or (i) the Disclosure Information specified in Section 3(c)(iii)(A) above for the first of the repetitive accountable disclosures, (ii) the frequency, periodicity, or number of the repetitive accountable disclosures, and (iii) the date of the last of the repetitive accountable disclosures.

iv) Availability of Disclosure Information. Business Associate will maintain the Disclosure Information for at least 6 years following the date of the accountable disclosure to which the Disclosure Information relates.

Business Associate will make the Disclosure Information available to Health Plan within 59 calendar days following Health Plan's request for such Disclosure Information to comply with an individual's request for disclosure accounting.

d) Restriction Agreements and Confidential Communications. Business Associate will comply with any agreement that Health Plan makes that either (i) restricts use or disclosure of Health Plan's Protected Health Information pursuant to 45 C.F.R. § 164.522(a), or (ii) requires confidential communication about Health Plan's Protected Health Information pursuant to 45 C.F.R. § 164.522(b), provided that Health Plan notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Health Plan will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Health Plan's Protected Health Information will remain subject to the terms of the restriction agreement.

4. Breaches and Security Incidents.

a) Reporting.

i) Privacy or Security Breach. Business Associate will report to Health Plan any use or disclosure of Health Plan's Protected Health Information not permitted by this Agreement or in writing by Health Plan, along with any Breach or possible Breach of Health Plan's Unsecured Protected Health Information. In connection with this report to Health Plan, Business Associate will prepare a written risk assessment for each Breach or possible Breach and shall provide a copy of such risk assessment to Health Plan. Business Associate will treat the Breach as being Discovered in accordance with HIPAA's requirements. Business Associate will make the report to Health Plan's Privacy Official not more than 59 calendar days after Business Associate learns of such non-permitted use or disclosure. If a delay is requested by a law enforcement official in accordance with 45 C.F.R. § 164.412, Business Associate may delay notifying Health Plan for the time period specified by such regulation. Business Associate's report will at least:

A) Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach;

B) Identify Health Plan's Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual-by-individual basis;

C) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;

D) Identify what corrective or investigational action Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;

E) Identify what steps the individuals who were subject to a Breach should take to protect themselves;

F) Provide such other information, including a written report, as Health Plan may reasonably request.

ii) Security Incidents. Business Associate will report to Health Plan within *15* calendar days any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of Health Plan's Electronic Protected Health Information or (B) interference with Business Associate's system operations in Business Associate's information systems, of which Business Associate becomes aware. Business Associate will make this report upon Health Plan's request, except if any such security incident resulted in a disclosure or Breach of Health Plan's Protected Health Information or Electronic Protected Health Information not permitted by this Agreement, Business Associate will make the report in accordance with Section 4(a)(i) above.

b) Termination of Agreement.

i) Termination Resulting from the End of Relationship, Functions or Services. This Agreement shall terminate in the event that the underlying relationship, functions, or services that give rise to the necessity of a Business Associate Agreement terminate for any reason.

ii) Right to Terminate for Breach. Health Plan may terminate Agreement if it determines, in its sole discretion, that Business Associate has breached any provision of this Agreement. Health Plan may exercise this right to terminate Agreement by providing Business Associate written notice of termination. Any such termination will be effective immediately or at such other date specified in Health Plan's notice of termination.

iii) Obligations on Termination.

A) Return or Destruction of Health Plan's Protected Health Information as Feasible. Upon termination or other conclusion of Agreement, Business Associate will, if feasible, return to Health Plan or destroy all of Health Plan's Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Health Plan's Protected Health Information. Business Associate will require any subcontractor or agent, to which Business Associate has disclosed Health Plan's Protected Health Information as permitted by Section 1(e) of this Agreement, to if feasible return to Business Associate (so that Business Associate may return it to Health Plan) or destroy all of Health Plan's Protected Health Information in whatever form or medium received from Business Associate, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Health Plan's Protected Health Information, and certify on oath to Business Associate that all such information has been returned or destroyed. Business Associate will

complete these obligations as promptly as possible, but not later than 30 calendar days following the effective date of the termination or other conclusion of Agreement.

B) Procedure When Return or Destruction Is Not Feasible. Business Associate will identify any of Health Plan's Protected Health Information, including any that Business Associate has disclosed to subcontractors or agents as permitted by Section 1(e) of this Agreement, that cannot feasibly be returned to Health Plan or destroyed and explain why return or destruction is infeasible. Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will require such subcontractor or agent to limit its further use or disclosure of Health Plan's Protected Health Information that such subcontractor or agent cannot feasibly return or destroy to those purposes that make the return or destruction of such information infeasible. Business Associate will complete these obligations as promptly as possible, but not later than *30* calendar days following the effective date of the termination or other conclusion of Agreement.

C) Continuing Privacy and Security Obligation. Business Associate's obligation to protect the privacy and safeguard the security of Health Plan's Protected Health Information as specified in this Agreement will be continuous and survive termination or other conclusion of this Agreement.

5. General Provisions.

a) Inspection of Internal Practices, Books, and Records. Business Associate will make its internal practices, books, and records relating to its use and disclosure of Health Plan's Protected Health Information available to Health Plan and to DHHS to determine Health Plan's compliance with the Privacy Rule, 45 C.F.R. Part 164, Subpart E.

b) Definitions. All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance. For purposes of this Agreement, Health Plan's Protected Health Information encompasses Health Plan's Electronic Protected Health Information.

c) Amendment to Agreement. Upon the compliance date of any final regulation or amendment to final regulation promulgated by DHHS that affects Business Associate's use or disclosure of Health Plan's Protected Health Information or Standard Transactions this Agreement will automatically amend such that the obligations imposed on Business Associate remain in compliance with the final regulation or amendment to final regulation.

d) No Third Party Beneficiaries. Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.

e) Delegation to Business Associate. To the extent the parties agree that Business Associate will carry out directly one or more of Health Plan's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Health Plan in the performance of such obligations**.**

f) No Agency Relationship. Both parties agree that Business Associate is not, and shall not be deemed to be, an agent of Health Plan.

IN WITNESS WHEREOF, Health Plan and Business Associate execute this Agreement in multiple originals to be effective, *December 1, 2025*.

By: loanDepot.com , LLC_____

Its: _____

Date: February 14, 2026_____

By: Anthem_____

Its: _____

Date: February 14, 2026_____

Business Associate Agreement Checklist

Purpose: The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was amended in 2009 by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). HIPAA and the HITECH Act require that a "covered entity" enter into a business associate agreement ("BAA") with a business associate. This Checklist discusses which terms must be included in a BAA. This Checklist also discusses some optional terms which covered entities and business associates may want to consider.

Mandatory Terms	**Check if Included / Comments**
1. Permitted Uses. The BAA must establish the permitted and required uses and disclosures of protected health information ("PHI") by the business associate.	☐ _____
2. Use of PHI by Business Associate. The BAA may not authorize the business associate to use or further disclose PHI in a manner that would violate the requirements of the Privacy Rule, if done by the covered entity. However, the BAA may permit: **a)** The business associate to use or disclose PHI for the business associate's proper management and administration (in limited circumstances); and **b)** The business associate to perform data aggregation services relating to a covered entity's health care operation. In addition, the BAA may allow the business associate to disclose such PHI if: **a)** the disclosure is required by law; or **b)** **(i)** the business associate obtains reasonable assurance from any person or entity to which the business associate will disclose the PHI that the person or entity will hold the PHI in confidence and use or further disclose PHI only for the purpose for which the business associate disclosed the PHI or as required by law; and **(ii)** the person notifies the business associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.	☐ _____
3. Follow BAA and HIPAA. The business associate will not use or further disclose the information other than as permitted or required by the BAA or as required by law.	☐ _____
4. Safeguards of PHI. The business associate must use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the BAA.	☐ _____

Mandatory Terms	Check if Included / Comments
5. Comply with HIPAA Security. The business associate must comply with the applicable requirements of the Security Rule, 45 CFR Part 164, Subpart C, including using appropriate safeguards for electronic PHI ("ePHI").	☐ _____
6. Reporting Improper Use or Disclosure. The business associate must report to the covered entity any use or disclosure of PHI not provided for by the BAA of which it becomes aware.	☐ _____
7. Report Security Incidents. The business associate must report to the covered entity any security incident of which it becomes aware.	☐ _____
8. Mitigation. The business associate must mitigate, to the extent practicable, any harmful effect that is known to the business associate of a use or disclosure of PHI by the business associate in violation of the requirements of the BAA.	☐ _____
9. Restrictions on Subcontractors. The business associate must ensure that any subcontractor, to whom the business associate provides PHI received from, or created or received by, the business associate on behalf of the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information.	☐ _____
10. Safeguards of Subcontractors. The business associate must ensure that any subcontractor, to whom the business associate provides ePHI agrees to implement reasonable and appropriate safeguards to protect such ePHI.	☐ _____
11. Access Rights. The business associate must make available PHI in accordance with an individual's access rights under 45 C.F.R. § 164.524 and the HITECH Act. The BAA should require that copies be available in electronic form.	☐ _____
12. Disclosure Accounting. The business associate must make available the information required to provide an accounting of the disclosures in accordance with 45 CFR § 164.528 and the HITECH Act.	☐ _____
13. Make Records Available. The business associate must make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by, the business associate, on behalf of the covered entity, available to the Secretary of the Department of Health and Human Services for purposes of determining the covered entity's compliance with HIPAA.	☐ _____
14. Return or Destroy PHI. The business associate must, upon termination of the BAA, return or destroy the PHI it received pursuant to the agreement, if feasible. For PHI which Business Associate cannot feasibly return or destroy, Business Associate must promise to continue to safeguard the PHI and use or disclose it only for the reasons that make return or destruction infeasible.	☐ _____
15. Report Breach. The business associate must report to the covered entity any breach of unsecured PHI in accordance with 45 C.F.R. Part 164 Subpart D. The business associate likely should	☐ _____

Mandatory Terms	Check if Included / Comments
include a copy of its risk assessment demonstrating why it was or was not a breach.	
16. <u>No Remuneration</u>. The business associate must not directly or indirectly receive remuneration in exchange for any PHI of an individual. Note: Technically remuneration would be possible with an authorization and satisfaction of some additional terms. However, this is not detailed here as this would presumably be rare (many covered entities may not allow it, even if allowed by law).	☐ _____ _____ _____
17. <u>Termination Upon Violation</u>. The business associate must permit the covered entity to terminate the BAA in case of material violation of a privacy or security provision of the BAA.	☐ _____ _____ _____
18. <u>Standard Transactions</u>. The business associate must comply with the Administrative Requirements of 45 C.F.R. Part 162 when acting on behalf of the covered entity. These requirements include, but are not limited to: • The business associate must comply with the Electronic Standard Transaction rules when the business associate conducts a Transaction described in 45 C.F.R. Part 162; • The business associate must not enter into a trading partner agreement on behalf of the covered entity that would violate 45 C.F.R. §162.915; • The business associate must comply with the National Provider Identification requirements contained in 45 C.F.R. §162.412; • The business associate must comply with all operating rules that apply to the covered entity, including but not limited to 45 C.F.R. §162.1403. Note that these provisions may not be required to be included in the BAA if the business associate will never engage in such transactions. However, the covered entity likely cannot know with certainty whether this would always be true in the future. Thus, the terms likely should be included in the BAA.	☐ _____ _____ _____
19. <u>Minimum Necessary</u>. The business associate must comply with the "minimum necessary" rules (including the requirement that the business associate limit the information to a "limited data set" to the extent practicable) when using, disclosing or requesting PHI, except when a specific exception applies under HIPAA or the HITECH Act.	☐ _____ _____ _____
20. <u>Amendment of PHI</u>. The business associate must make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. §162.526.	☐ _____ _____ _____
21. <u>Carrying Out Plan's Obligations</u>. To the extent the business associate will carry out a plan's obligation under the HIPAA Privacy Rules, the business associate must comply with the Privacy Rule requirements that apply to the plan.	☐ _____ _____ _____

Mandatory Terms	Check if Included / Comments
22. Comply with Reproductive Health Care Regulations. The BAA should ensure that the business associate complies with the April 2024 HIPAA regulations related to reproductive health care.	☐ _____ _____ _____

Strongly Suggested / Typically Included Provisions	Check if Included / Comments
1. Termination Due to Overall Relationship Ending. The BAA shall terminate in the event that the underlying relationship, functions, or services that gives rise to the necessity of a BAA terminates for any reason.	☐ _____ _____ _____
2. Reporting of Violation. The business associate may use PHI to report violations of law to the appropriate state and federal authorities, consistent with 45 CFR § 164.502(j)(i).	☐ _____ _____ _____
3. Restriction Requests. The covered entity shall notify the business associate of any restriction to the use or disclosure of PHI that the covered entity has agreed to in accordance with 45 CFR § 164.522(a) and the HITECH Act.	☐ _____ _____ _____
4. Confidential Communication Requests. The covered entity shall notify the business associate of any confidential communication requests which the covered entity has agreed to in accordance with 45 CFR § 164.522(b).	☐ _____ _____ _____
5. Who Determines Breach. Describe which entity (the plan or business associate) will determine whether a breach occurred.	
6. Other Terms. Non-HIPAA, "standard" contract terms such as: * Severability -- if one section is invalid, the rest remain * Section headings are for convenience only * Notices must be in writing * Waiver of one provision of the BAA does not waive other provisions * BAA drafted by all parties * Applicable law and venue * BAA may be executed in multiple counterparts * No Sending PHI or ePHI to locations outside United States * Business associate is not an "agent" of the plan	☐ _____ _____ _____

Use Caution Regarding These Terms	Check if Included / Comments
1. Indemnification. Indemnification (especially if one-sided and not mutual).	☐ _____ _____
2. Reference to Other Documents. Requirement to follow the other party's notice of privacy practices or policies and procedures.	☐ _____ _____ _____

loanDepot.com LLC Welfare Benefits Plan
AUTHORIZATION

Purpose: This form is used for an individual to authorize use or disclosure of the individual's protected health information for the purposes stated.

SECTION A: Psychotherapy notes.

☐ Check if this authorization is for psychotherapy notes.

If this authorization is for psychotherapy notes, you must *not* use it as an authorization for any other type of protected health information.

SECTION B: Individual authorizing use and/or disclosure.

Name: _____

Address: _____

Telephone: _____ E-mail: _____

Identification Number: _____

TO THE INDIVIDUAL: Please read the following and complete the information requested.

No Conditions: This authorization is voluntary. We will not condition your enrollment in a health plan or eligibility for benefits on receiving this authorization.

Effect of Granting this Authorization: The protected health information described below may be disclosed to and/or received by persons or organizations who are not subject to federal health information privacy laws. These persons or organizations may further disclose the protected health information, and it may no longer be protected by federal health information privacy laws.

SECTION C: The use and/or disclosure being authorized.

Purpose of this Authorization:

☐ At request of individual (or the individual's personal representative).

☐ For the following purposes:

_____

_____

Protected Health Information to Be Used and/or Disclosed: Specifically and meaningfully describe the protected health information that this authorization will allow to be used and/or disclosed:

_____

_____

Entities Authorized to Use or Disclose: Name or specifically describe the persons and/or organizations (or the classes of persons and/or organizations), including us, who will be authorized to make use of and/or to disclose the protected health information described above:

Entities Authorized to Receive and Use: Name or specifically identify the persons and/or organizations (or the classes of persons and/or organizations), including us, whom this authorization will allow to receive and use the protected health information described above:

SECTION D: Expiration and revocation.

Expiration: This authorization will expire (complete one):

☐ On _____/_____/_____

☐ On occurrence of the following event (which must relate to the individual or to the purpose of the use and/or disclosure being authorized):

Right to Revoke: You may revoke this authorization at any time by giving written notice of revocation to the Contact Office listed below. Revocation of this authorization will *not* affect any action we took in reliance on this authorization before we received your written notice of revocation.

Contact Office: _____

Telephone: _____ Fax: _____

E-mail: _____

Address: _____

INDIVIDUAL'S SIGNATURE.

I, _____, have had full opportunity to read and consider the contents of this authorization. I understand that, by signing this form, I am confirming my authorization for the use and/or disclosure of my protected health information, as described in this form.

Signature: _____ Date: _____

If this authorization is signed by a personal representative on behalf of the individual, complete the following:

Personal Representative's Name: _____

Relationship to Individual: _____

YOU ARE ENTITLED TO A COPY OF THIS AUTHORIZATION AFTER YOU SIGN IT.

Include this authorization in the individual's records.

Send copy to the Privacy Official.

PLAN DOCUMENT AMENDMENT

Purpose: The amendment in this Form is generally needed if the employer will receive protected health information while performing activities on behalf of the health plan. If we are completing this Form 4, we also must complete Form 5, Certification of Amendment and also must verify that Form 7, Privacy Practices Notice, states that disclosures to the employer are allowed.

loanDepot.com LLC Welfare Benefits Plan

GROUP HEALTH PLAN DOCUMENT AMENDMENT

ARTICLE ___
PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

1. loanDepot.com, LLC's Certification of Compliance.

Neither Plan nor any health insurance issuer or business associate servicing Plan will disclose Plan Participants' Protected Health Information to **loanDepot.com, LLC** unless **loanDepot.com, LLC** certifies that the Plan Document has been amended to incorporate this Article and agrees to abide by this Article.

2. Purpose of Disclosure to loanDepot.com, LLC.

Plan and any health insurance issuer or business associate servicing Plan will disclose Plan Participants' Protected Health Information to **loanDepot.com, LLC** only to permit **loanDepot.com, LLC** to carry out the following plan administration functions for Plan:

Claim assistance, work with the TPA to handle the appeal process and various other actions for the Plan Administrator.

Any disclosure to and use by **loanDepot.com, LLC** of Plan Participants' Protected Health Information will be subject to and consistent with the provisions of Sections 3 through 5 of this Article and the specifications and requirements of the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations ("C.F.R.") Parts 160-64.

(a) Neither Plan nor any health insurance issuer or business associate servicing Plan will disclose Plan Participants' Protected Health Information to **loanDepot.com, LLC** unless the disclosures are explained in the Privacy Practices Notice distributed to the Plan Participants.

(b) Neither Plan nor any health insurance issuer or business associate servicing Plan will disclose Plan Participants' Protected Health Information to **loanDepot.com, LLC** for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of **loanDepot.com, LLC**.

3. Restrictions on loanDepot.com, LLC's Use and Disclosure of Protected Health Information.

(a) **loanDepot.com, LLC** will neither use nor further disclose Plan Participants' Protected Health Information, except as permitted or required by the Plan Document, as amended by this Article, or as required by law.

(b) **loanDepot.com, LLC** will ensure that any agent, including any subcontractor, to which it provides Plan Participants' Protected Health Information agrees to the restrictions, conditions, and security measures of the Plan Document, as amended by this Article, with respect to Plan Participants' Protected Health Information.

(c) **loanDepot.com, LLC** will not use or disclose Plan Participants' Protected Health Information for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of **loanDepot.com, LLC**.

(d) **loanDepot.com, LLC** will report to Plan any use or disclosure of Plan Participants' Protected Health Information that is inconsistent with the uses and disclosures allowed under the Plan Document, as amended by this Article**,** promptly upon learning of such inconsistent use or disclosure.

(e) **loanDepot.com, LLC** will make Protected Health Information available to Plan or to the Plan Participant who is the subject of the information in accordance with 45 C.F.R. § 164.524.

(f) **loanDepot.com, LLC** will make Plan Participants' Protected Health Information available for amendment, and will on notice amend Plan Participants' Protected Health Information, in accordance with 45 C.F.R. § 164.526.

(g) **loanDepot.com, LLC** will track disclosures it may make of Plan Participants' Protected Health Information that are accountable under 45 C.F.R. § 164.528 so that it can make available the information required for Plan to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528.

(h) **loanDepot.com, LLC** will make its internal practices, books, and records relating to its use and disclosure of Plan Participants' Protected Health Information available to Plan and to the U.S. Department of Health and Human Services to determine Plan's compliance with the HIPAA Privacy Rule at 45 C.F.R. Part 164, Subpart E.

(i) **loanDepot.com, LLC** will, if feasible, return or destroy (and cause its subcontractors and agents to, if feasible, return or destroy) all Plan Participants' Protected Health Information, in whatever form or medium, received from Plan or any health insurance issuer or business associate servicing Plan, including all copies thereof and all data, compilations, or other works derived therefrom that allow identification of any Participant who is the subject of the Protected Health Information, when the Plan Participants' Protected Health Information is no longer needed for the plan administration functions for which the disclosure was made. If it is not feasible to return or destroy all Plan Participants' Protected Health Information, **loanDepot.com, LLC** will limit (and will cause its subcontractors and agents to limit) the use or disclosure of any Plan Participants' Protected Health Information that cannot feasibly be returned or destroyed to those purposes that make the return or destruction of the information infeasible.

4. Security Measures for Electronic Protected Health Information

(a) **loanDepot.com, LLC** will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Plan Participants' Electronic Protected Health Information that **loanDepot.com, LLC** creates, receives, maintains, or transmits on Plan's behalf.

(b) **loanDepot.com, LLC** will report to Plan, upon Plan's request, any attempted or successful (i) unauthorized access, use, disclosure, modification, or destruction of Plan Participants' Electronic Protected Health Information or (ii) interference with **loanDepot.com, LLC's** system operations in **loanDepot.com, LLC's** information systems, of which **loanDepot.com, LLC** becomes aware, except any such security incident that results in disclosure of Plan Participants' Protected Health Information not permitted by the Plan Document, as amended by this Article, must be reported to Plan as required by Paragraph 3(d), above.

(c) **loanDepot.com, LLC** will support the adequate separation between **loanDepot.com, LLC** and Plan, as specified by Section 5, below, with reasonable and appropriate security measures.

5. Adequate Separation Between loanDepot.com, LLC and Plan.

(a) The following employees or classes of employees or other workforce members under the control of **loanDepot.com, LLC** may be given access to Plan Participants' Protected Health Information received from Plan or a health insurance issuer or business associate servicing Plan:

_____	_____
_____	_____
_____	_____
_____	_____

This list includes every employee or class of employees or other workforce members under the control of **loanDepot.com, LLC** who may receive Plan Participants' Protected Health Information relating to payment under, the health care operations of, or other matters pertaining to Plan in the ordinary course of business.

(b) The employees, classes of employees or other workforce members identified in Paragraph 5(a), above will have access to Plan Participants' Protected Health Information only to perform the plan administration functions that **loanDepot.com, LLC** provides for Plan, as specified in Paragraph 2(a), above.

(c) The employees, classes of employees or other workforce members identified in Paragraph 5(a), above will be subject to disciplinary action and sanctions, including termination of employment or affiliation with **loanDepot.com, LLC**, for any use or disclosure of Plan Participants' Protected Health Information in breach or violation of or noncompliance with the provisions of this Article. **loanDepot.com, LLC** will promptly report such breach, violation or noncompliance to Plan, as required by Paragraph 3(d), above and will cooperate with Plan to correct the breach, violation or noncompliance, to impose appropriate disciplinary action or sanctions on each employee or other workforce member causing the breach, violation or noncompliance, and to mitigate any deleterious effect of the breach, violation or noncompliance on any Participant, the privacy of whose Protected Health Information may have been compromised by the breach, violation or noncompliance.

Adopted **February 14, 2026**

CERTIFICATION OF AMENDMENT

Purpose: We must complete the certification found in this Form if we have completed FORM 4 -- Plan Document Amendment.

loanDepot.com, LLC

{DATE}

{HEALTH PLAN'S NAME}
{HEALTH PLAN'S ADDRESS}

Re: Certification of Group Health Plan Document Amendment

Dear **{HEALTH PLAN}**:

loanDepot.com, LLC ("Plan Sponsor") is the sponsor of **loanDepot.com LLC Welfare Benefits Plan** ("Group Health Plan"). Plan Sponsor performs plan administration functions for Group Health Plan and needs access to the Group Health Plan participants' protected health information to carry out those plan administration functions.

Plan Sponsor hereby certifies that the plan document of Group Health Plan has been amended effective **{DATE}** to comply with the requirements of 45 Code of Federal Regulations § 164.504(f)(2). The amendment provides the required assurance that Plan Sponsor will appropriately safeguard and limit the use and disclosure of the Group Health Plan participants' protected health information that Plan Sponsor may receive from Group Health Plan or you to perform the plan administration functions.

Accordingly, please provide Plan Sponsor the minimum necessary protected health information of Group Health Plan participants for Plan Sponsor to perform the following plan administration functions:

x Claim assistance, work with the TPA to handle the appeal process and various other actions for the Plan Administrator

_____

_____

_____

Please provide this protected health information to the following individuals:

_____
_____

_____
_____

_____
_____

_____
_____

Sincerely,

loanDepot.com, LLC

By: _____

Its: _____

loanDepot.com LLC Welfare Benefits Plan

DISCLOSURE LOG/MINIMUM NECESSARY

Purpose: This form is used to document each disclosure of protected health information that we make for which we are obligated to account on an individual's request. This form is also used to document our compliance with the minimum necessary requirement.

SECTION A: Individual whose protected health information was disclosed.

Name: _____

Address: _____

Telephone: _____ E-mail: _____

Identification Number: _____

SECTION B: Disclosure made.

Disclosure Date: _____/_____/_____

Name and Address (if known) of Person or Entity to whom the Protected Health Information Was Disclosed: _____

_____

Protected Health Information Disclosed: _____

_____

_____

Purpose of the Disclosure: Describe the purpose for disclosing the protected health information, or attach a copy of any written request for the information received from a government agency.

_____

_____

Repetitive Disclosure:

☐ Check if this disclosure is one of a series of repetitive accountable disclosures for a single purpose to the same person or entity. State, if known, the date of the first disclosure of the series, and the frequency, periodicity or number of these repetitive disclosures made prior to the disclosure being reported on this form.

_____

_____

SECTION C: Minimum necessary determination (check each applicable box).

☐ No minimum necessary determination was required because:

- ☐ Disclosure was to a health care provider to carry out treatment.
- ☐ Disclosure was to the individual in Section A or to that individual's personal representative.
- ☐ Disclosure was authorized by the individual in Section A or that individual's personal representative. Attach the authorization.
- ☐ Disclosure was to the Department of Health and Human Services for compliance review or complaint investigation or enforcement.
- ☐ Disclosure was required by law. Cite the law: _____
- ☐ Disclosure was required for compliance with HIPAA Administration Simplification Rules. Cite the Rule and why disclosure was required to comply with it: _____

  _____

  .
- ☐ Disclosure was to a covered entity whose request appeared reasonable under the circumstances.
- ☐ Disclosure was to a public official whose representation that the minimum necessary was requested appeared reasonable under the circumstances.
- ☐ Disclosure was to a professional who is a member of our workforce or our business associate, and whose representation that the minimum necessary was requested appeared reasonable under the circumstances.
- ☐ Disclosure was to a researcher providing appropriate documentation to support that the disclosure was the minimum necessary.

☐ This disclosure was part of a series of routine or recurring disclosures and was made in accordance with our standard protocols that limit such disclosures to the minimum reasonably necessary for the purpose.

☐ This disclosure was the minimum reasonably necessary based on an individualized determination made by applying our criteria for limiting such disclosures to the minimum necessary for the purpose. Identify the person who made the individualized determination: _

☐ This disclosure was for an entire medical record. State the justification for the entire medical record being the minimum necessary protected health information for the purpose: _____

_____

SIGNATURE.

I attest that the above information is correct.

Signature: _____ Date: _____

Print name: _____ Title: _____

Include completed form in the individual's records.
Send copy to the Privacy Official.

PRIVACY PRACTICES NOTICE

loanDepot.com LLC Welfare Benefits Plan

PRIVACY PRACTICES NOTICE

(Version 02/16/2026)

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. THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

{The following summary section is optional, though suggested by HHS for a "layered notice" at 67 Fed. Reg. 53243 (Aug. 14. 2002) and 78 Fed. Reg. 5625 (Jan. 25, 2013).}

Summary of Our Privacy Practices

We may use and disclose your protected health information ("medical information"), without your permission, for treatment, payment, and health care operations activities. We may use and disclose your medical information, without your permission, when required or authorized by law for public health activities, law enforcement, judicial and administrative proceedings, research, and certain other public benefit functions.

We may disclose your medical information to your family members, friends, and others you involve in your care or payment for your health care. We may disclose your medical information to appropriate public and private agencies in disaster relief situations.

We may disclose to your employer whether you are enrolled or disenrolled in the health plans it sponsors. We may disclose summary health information to your employer for certain limited purposes. We may disclose your medical information to your employer to administer your group health plan if your employer explains the limitations on its use and disclosure of your medical information in the plan document for your group health plan.

Except for certain legally-approved uses and disclosures, we will not otherwise use or disclose your medical information without your written authorization.

You have the right to examine and receive a copy of your medical information. You have the right to receive an accounting of certain disclosures we may make of your medical information. You have the right to request that we amend, further restrict use and disclosure of, or communicate in confidence with you about your medical information.

You have the right to receive notice of breaches of your unsecured medical information.

Please review this entire notice for details about the uses and disclosures we may make of your medical information, about your rights and how to exercise them, and about complaints regarding or additional information about our privacy practices.

Contact Information

For more information about our privacy practices, to discuss questions or concerns, or to get additional copies of this notice, please contact our Contact Office. **liveWell@loandepot.com**

Contact Office: Benefits Department, Irvine, CA

Telephone: (949) 465-8414 Fax: (949) 575-5349 E-mail: liveWell@loandepot.com

Address: 6561 Irvine Center Drive
Irvine, CA 92618

Health Plans Covered by this Notice

This notice applies to the privacy practices of the health plans listed below. They may share with each other your medical information, and the medical information of others they service, for the health care operations of their joint activities.

Medical

Health Flexible Spending Account

Our Legal Duty

We are required by applicable federal and state law to maintain the privacy of your protected health information ("medical information"). We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your medical information.

We must follow the privacy practices that are described in this notice while it is in effect. This notice takes effect **February 16, 2026**, and will remain in effect unless we replace it.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided such changes are permitted by applicable law. We reserve the right to make any change in our privacy practices and the new terms of our notice applicable to all medical information we maintain, including medical information we created or received before we made the change.

Uses and Disclosures of Your Medical Information

Treatment: We may disclose your medical information, without your permission, to a physician or other health care provider to treat you.

Payment: We may use and disclose your medical information, without your permission, to pay claims from physicians, hospitals and other health care providers for services delivered to you that are covered by your health plan, to determine your eligibility for benefits, to coordinate your benefits with other payers, to determine the medical necessity of care delivered to you, to obtain premiums for your health coverage, to issue explanations of benefits to the subscriber of the health plan in which you participate, and the like. We may disclose your medical information to a health care provider or another health plan for that provider or plan to obtain payment or engage in other payment activities.

Health Care Operations: We may use and disclose your medical information, without your permission, for health care operations. Health care operations include:

- health care quality assessment and improvement activities;
- reviewing and evaluating health care provider and health plan performance, qualifications and competence, health care training programs, health care provider and health plan accreditation, certification, licensing and credentialing activities;
- conducting or arranging for medical reviews, audits, and legal services, including fraud and abuse detection and prevention;
- underwriting and premium rating our risk for health coverage, and obtaining stop-loss and similar reinsurance for our health coverage obligations; and
- business planning, development, management, and general administration, including customer service, grievance resolution, claims payment and health coverage improvement activities, de-identifying medical information, and creating limited data sets for health care operations, public health activities, and research.

We may disclose your medical information to another health plan or to a health care provider subject to federal privacy protection laws, as long as the plan or provider has or had a relationship with you and the medical information is for that plan's or provider's health care quality assessment and improvement activities, competence and qualification evaluation and review activities, or fraud and abuse detection and prevention.

Your Authorization: You may give us written authorization to use your medical information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosure permitted by your authorization while it was in effect. Unless you give us a written authorization, we will not use or disclose your medical information for any purpose other than those described in this notice. We generally may use or disclose any psychotherapy notes and substance use disorder counseling notes we hold only with your authorization.

If we receive substance use disorder treatment records created by a federally assisted program or health care provider under 42 CFR Part 2, we may only use or disclose such records in accordance with the written consent you provided to the program or provider. If such records were disclosed to us with your written consent for treatment, payment, and health care operations, we may further disclose the records for these purposes without obtaining an additional written consent.

Family, Friends, and Others Involved in Your Care or Payment for Care: We may disclose your medical information to a family member, friend or any other person you involve in your care or payment for your health care. We will disclose only the medical information that is relevant to the person's involvement.

We may use or disclose your name, location, and general condition to notify, or to assist an appropriate public or private agency to locate and notify, a person responsible for your care in appropriate situations, such as a medical emergency or during disaster relief efforts.

We will provide you with an opportunity to object to these disclosures, unless you are not present or are incapacitated or it is an emergency or disaster relief situation. In those situations, we will use our professional judgment to determine whether disclosing medical information related to your care or payment is in your best interest under the circumstances.

Your medical information remains protected by us for at least 50 years after you die. After you die, we may disclose to a family member, or other person involved in your health care prior to your death, the medical information that is relevant to that person's involvement, unless doing so is inconsistent with your preference and you have told us so.

Your Employer: We may disclose to your employer whether you are enrolled or disenrolled in a health plan that your employer sponsors.

We may disclose summary health information to your employer to use to obtain premium bids for the health insurance coverage offered under the group health plan in which you participate or to decide whether to modify, amend or terminate that group health plan (this is sometimes called "underwriting"). Summary health information is aggregated claims history, claims expenses or types of claims experienced by the enrollees in your group health plan. Although summary health information will be stripped of all direct identifiers of these enrollees, it still may be possible to identify medical information contained in the summary health information as yours. We are expressly prohibited from using or disclosing any health information containing your genetic information for underwriting purposes.

{We may disclose your medical information and the medical information of others enrolled in your group health plan to your employer to administer your group health plan. Before we may do that, your employer must amend the plan document for your group health plan to establish the limited uses and disclosures it may make of your medical information. Please see your group health plan document for a full explanation of those limitations.}

Health-Related Products and Services: We may use your medical information to communicate with you about health-related products, benefits and services, and payment for those products, benefits and services that we provide or include in our benefits plan. We may use your medical information to communicate with you about treatment alternatives that may be of interest to you.

These communications may include information about the health care providers in our networks, about replacement of or enhancements to your health plan, and about health-related products or services that are available only to our enrollees that add value to our benefits plans.

Public Health and Benefit Activities: We may use and disclose your medical information, without your permission, when required by law, and when authorized by law for the following kinds of public health and public benefit activities:

- for public health, including to report disease and vital statistics, child abuse, and adult abuse, neglect or domestic violence;
- to avert a serious and imminent threat to health or safety;
- for health care oversight, such as activities of state insurance commissioners, licensing and peer review authorities, and fraud prevention agencies;
- for research;
- in response to court and administrative orders and other lawful process;
- to law enforcement officials with regard to crime victims and criminal activities;
- to coroners, medical examiners, funeral directors, and organ procurement organizations;
- to the military, to federal officials for lawful intelligence, counterintelligence, and national security activities, and to correctional institutions and law

enforcement regarding persons in lawful custody; and
- as authorized by state worker's compensation laws.

Prohibited Uses and Disclosures: If we receive substance use disorder records created by a federally assisted program or health care provider under 42 CFR Part 2, we may not use or disclose such records, or testimony relaying the content of such records, in any civil, criminal, administrative, or legislative proceedings against you unless based on your specific written consent or a court order. We may only use or disclose records based on a court order after:

1. a notice and an opportunity to be heard is provided to you or the holder of the record, where required by 42 CFR part 2; and

2. the court order is accompanied by a subpoena or other similar legal requirement compelling the disclosure.

Your Rights

Access: You have the right to examine and to receive a copy of your medical information, with limited exceptions. You should submit your request **{in writing}** to our Contact Office.

{We may charge you reasonable, cost-based fees (including labor costs) for a copy of your medical information, for mailing the copy to you, and for preparing any summary or explanation of your medical information you request. Contact our Contact Office for information about our fees.}

Your medical information may be maintained electronically. If so, you can request an electronic copy of your medical information. If you do, we will provide you with your medical information in the electronic form and format you requested, if it is readily producible in such form and format. If not, we will produce it in a readable electronic form and format as we mutually agree upon.

You may request that we transmit your medical information directly to another person you designate. If so, we will provide the copy to the designated person. Your request must be in writing, signed by you and must clearly identify the designated person and where we should send the copy of your medical information.

Disclosure Accounting: You have the right to a list of instances from the prior six years **{if plan is created after that date, insert the effective date}** in which we disclose your medical information for purposes other than treatment, payment, health care operations, as authorized by you, and for certain other activities.

You should submit your request to the contact at the end of this notice. We will provide you with information about each accountable disclosure that we made during the period for which you request the accounting, except we are not obligated to account for a disclosure that occurred more than 6 years before the date of your request and never for a disclosure that occurred before the plan's effective date (if the plan was created less than six years ago).

Amendment. You have the right to request that we amend your medical information. You should submit your request **{in writing}** to the contact at the end of this notice.

We may deny your request only for certain reasons. If we deny your request, we will provide you a written explanation. If we accept your request, we will make your amendment part of your medical information and use reasonable efforts to inform others of the amendment who we know may have

and rely on the unamended information to your detriment, as well as persons you want to receive the amendment.

Restriction: You have the right to request that we restrict our use or disclosure of your medical information for treatment, payment or health care operations, or with family, friends or others you identify. We are not required to agree to your request, except for certain required restrictions, described below. If we do agree, we will abide by our agreement, except in a medical emergency or as required or authorized by law. You should submit your request to the contact at the end of this notice. We will agree to (and not terminate) a restriction request if:

1. the disclosure is to a health plan for purposes of carrying out payment or health care operations and is not otherwise required by law; and

2. the medical information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

Confidential Communication: You have the right to request that we communicate with you about your medical information in confidence by means or to locations that you specify. **{You should make your request in writing, and your request must represent that the information could endanger you if it is not communicated in confidence as you request.}** You should submit your request **{in writing}** to the contact at the end of this notice.

We will accommodate your request if it is reasonable, specifies the means or location for communicating with you, and continues to permit us to collect premiums and pay claims under your health plan. Please note that an explanation of benefits and other information that we issue to the subscriber about health care that you received for which you did not request confidential communications, or about health care received by the subscriber or by others covered by the health plan in which you participate, may contain sufficient information to reveal that you obtained health care for which we paid, even though you requested that we communicate with you about that health care in confidence.

Breach Notification: You have the right to receive notice of a breach of your unsecured medical information. Notification may be delayed or not provided if so required by a law enforcement official. You may request that notice be provided by electronic mail. If you are deceased and there is a breach of your medical information, the notice will be provided to your next of kin or personal representatives if the plan knows the identity and address of such individual(s).

Electronic Notice: If you receive this notice on our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact our Contact Office to obtain this notice in written form.

Complaints

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about access to your medical information, about amending your medical information, about restricting our use or disclosure of your medical information, or about how we communicate with you about your medical information (including a breach notice communication), you may complain to our Contact Office.

You also may submit a written complaint to the Office for Civil Rights of the United States Department of Health and Human Services, 200 Independence Avenue, SW, Room 509F, HHH Building, Washington,

D.C. 20201. You may contact the Office for Civil Rights' Hotline at 1-800-368-1019.

We support your right to the privacy of your medical information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

loanDepot.com LLC Welfare Benefits Plan

PRIVACY TRAINING CERTIFICATE

Purpose: This form is used to certify completion of privacy training by a workforce member. Retain the form for at least six years from the date noted below.

Section A—Workforce member trained.

Name: _____

Department: _____

Job Title: _____

Work Address: _____

Telephone: _____ E-mail: _____

Employee ID: _____

Date privacy training completed: ____/____/_____ Privacy training hours: _____

Reason for privacy training: _____

SIGNATURE OF PRIVACY INSTRUCTOR.

I attest that the above information is correct.

Signature: _____ Date: _____

Print name: _____ Title: _____

SECTION B—Workforce member's training acknowledgement.

I attest that I completed training on our health plan's privacy policies and procedures as set out above.

Signature: _____ Date: _____

Print name: _____ Title: _____

loanDepot.com LLC Welfare Benefits Plan

DESIGNATED PERSONNEL AND RECORD SETS

Purpose: This form is used to document the designation of personnel responsible for compliance with individuals' requests for access to, amendment of, and disclosure accounting for their protected health information, and the locations and electronic paths of documentation that makes up our designated record sets. Our designated record sets consist of all documentation that we maintain or that our agents/subcontractors maintain for us that makes up our enrollment, payment, claims adjudication, and case or medical management record systems, as well as all documentation that is used to make decisions about our enrollees. Note that it is possible that we will have little (or none) of this information on-site. For example, our health plan's third party administrator may have all of this information.

SECTION A: Department.

Name: _____

Director: _____

Location: _____

Mail Stop: _____ E-mail: _____

Telephone: _____ Fax: _____

SECTION B: Designated personnel.

The following department personnel or positions are responsible for the department's compliance with requests for access to, amendment of, and disclosure accounting for protected health information:

_____ _____

SECTION C: Designated record sets.

The file drawers and room locations of paper documentation that is part of the department's designated record sets:

_____ _____

_____ _____

The paths to electronic documentation that is part of the department's designated record sets:

_____ _____

_____ _____

An individual's protected health information may best be retrieved from the department's designated record sets by:

☐ Individual's name
☐ Identification number
☐ Social Security Number
☐ Other identifiers: _____