



Policy Name: Notice of Privacy Practices (NPP)

Policy Number	ADM-151	Version	002
Drafted By	Cynthia Donate	Effective Date	07/16/2025
Responsible Person	Business Manager	Next Review Date	03/01/2026

1. Purpose

Apple Specialty Pharmacy (“ASP”) is committed to protecting the privacy and security of Protected Health Information (“PHI”) and other personal information collected from individuals in the course of our pharmacy operations, in compliance with applicable federal and California state laws and regulations.

This policy also serves as Apple Specialty Pharmacy’s Notice of Privacy Practices (NPP) under HIPAA. It informs individuals about their rights regarding their Protected Health Information (PHI), how ASP may use and disclose their PHI, and ASP’s legal duties as a HIPAA-covered entity.

This policy establishes how ASP collects, uses, discloses, and protects PHI and other personal information, and ensures compliance with:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act)
- The Federal Trade Commission Act (FTC Act)
- California Confidentiality of Medical Information Act (CMIA)
- California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA)
- California Online Privacy Protection Act (CalOPPA)
- California Data Breach Notification Law
- Other applicable federal and state laws and regulations

2. Scope

This policy applies to all PHI and personal information ASP collects, maintains, processes, or discloses, including information obtained via:

- ASP’s website: <https://applespecialtypharmacy.com/>
- Pharmacy services and operations
- Communication channels (telephone, email, SMS, mail, in-person interactions)
- Third-party vendors or business associates acting on ASP’s behalf

3. Definitions

- PHI (Protected Health Information): Individually identifiable health information maintained or transmitted in any form, as defined under 45 C.F.R. § 160.103.
- Personal Information: Information that identifies, relates to, describes, or could reasonably be linked to a particular consumer or household (per CCPA/CPRA).
- Business Associate: A person or entity performing functions involving PHI on behalf of ASP, as defined in 45 C.F.R. § 160.103.

4. Policy

4.1 Collection of Information

Apple Specialty Pharmacy is a HIPAA-covered entity and complies with all applicable federal and state privacy laws in its collection and handling of PHI.

ASP may collect:

- PHI, including but not limited to:
 - Patient names, addresses, contact details
 - Medical histories, diagnoses, medications
 - Insurance and payment information
- Personal Information not constituting PHI, including:
 - Website usage data (e.g., IP address, browser type, pages visited)
 - Communications via online forms or email
 - Cookies and other tracking technologies as required under CalOPPA

ASP's website privacy practices are disclosed publicly per CalOPPA requirements.

4.2 Use of Information

ASP uses PHI and personal information for:

- Treatment, payment, and healthcare operations as permitted under HIPAA (45 C.F.R. §§ 164.502, 164.506)
- Pharmacy services, including prescription processing, patient counseling, and medication management
- Customer service and communications
- Compliance with legal or regulatory obligations
- Website analytics and improvement

- Marketing communications consistent with HIPAA and CAN-SPAM Act requirements, with appropriate authorizations if required

4.3 Disclosure of Information

ASP may disclose PHI and personal information as permitted or required under:

- HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E)
- CMIA (Cal. Civ. Code §§ 56-56.37)
- CCPA/CPRA for non-PHI personal data
- FTC Act § 5 prohibitions on deceptive practices
- California Data Breach Notification Law (Cal. Civ. Code §§ 1798.29, 1798.82)

Examples of permissible disclosures:

- To healthcare providers for treatment
- To insurers for billing purposes
- To government authorities for public health reporting
- To law enforcement as required by law
- To patients themselves upon request, consistent with HIPAA access rights

ASP does not sell PHI or personal information.

4.4 Individual Rights

Under HIPAA

Patients have rights under 45 C.F.R. § 164.520, including:

- Right to access their PHI
- Right to request corrections to their records
- Right to request an accounting of disclosures
- Right to request restrictions on use/disclosure
- Right to receive confidential communications
- Right to receive a copy of this Notice of Privacy Practices (NPP): Patients may request a paper or electronic copy of this notice at any time, even if they have agreed to receive it electronically. ASP will provide the requested copy promptly.

Under California Law (CCPA/CPRA)

California residents have rights under Cal. Civ. Code § 1798.100 et seq., including:

- Right to know what personal information is collected and how it's used
- Right to request deletion of personal information
- Right to correct inaccurate personal information
- Right to opt out of the sale or sharing of personal information (not applicable to PHI under HIPAA)

- Right to limit use of sensitive personal information

4.5 Data Security

ASP implements administrative, physical, and technical safeguards as required under:

- HIPAA Security Rule (45 C.F.R. §§ 164.302–164.318)
- HITECH Act
- Cal. Civ. Code §§ 1798.81.5, 1798.82 (CA Data Breach Notification)

4.6 Breach Notification

ASP shall notify affected individuals, the Department of Health and Human Services (HHS), and other regulatory bodies in the event of a breach of PHI, consistent with:

- HIPAA Breach Notification Rule (45 C.F.R. §§ 164.400–414)
- California Data Breach Notification Law (Cal. Civ. Code §§ 1798.29, 1798.82)

4.7 Website Privacy Policy Posting

The website privacy notice complements, but does not replace, this HIPAA Notice of Privacy Practices. Individuals may by submitting a request through any listed contact method listed below in “7. Contact.”

ASP shall maintain a publicly accessible Privacy Policy on its website, in compliance with:

- CalOPPA (Cal. Bus. & Prof. Code §§ 22575–22579)
- CCPA/CPRA for website data practices
- FTC Act requirements for truthful representations

5. Training

All employees shall receive training on privacy practices upon hire and annually thereafter, in compliance with HIPAA and California law.

6. Enforcement and Discipline

Violations of this policy may result in disciplinary action, up to and including termination. Contractors or vendors found to violate this policy may be subject to contract termination and potential legal action.

7. Contact

Direct questions regarding this policy and/or requests to exercise privacy rights to the Privacy Officer:

Written requests should be sent to:

Apple Specialty Pharmacy
1211 N. Broadway, Ste 300
Santa Ana, CA 92701

-or-

Email: privacy@applespecialtypharmacy.com

-or-

Fax: 323-955-2775

Verbal requests can be initiated via call to:

Phone: 323-999-2775

Heading	Definition
Policy Number	Each policy document has a unique number, starting at 001. This is referred to in the contents page of the policy manual.
Policy Name	A few unique words that describe the general subject matter of the policy.
Version Number	When a policy is being drafted, its Version Number is "000". Once passed at a GM, it becomes version "001". Following scheduled or other revisions, this number increases by one.
Drafted By	The person, group of people, subcommittee, etc., that drafted the policy. These people may be contacted prior to any future changes being made, or regarding any confusion around the original intent of the policy.
Responsible Person:	Person or position responsible for day-to-day implementation of policy.
Next Review Date:	The date set by the Board for review of the policy. If left blank or "n/a", the policy will be reviewed two years from the date of approval, or whenever the Board determines that a need has arisen. Reviews must follow the same development procedure as new policy proposals.
Purpose	What this policy seeks to achieve.
Policy	The actual content of the policy; the details of the position held by the organisation on the topic. A policy document may include several sub-headings under this topic, depending on the complexity of the policy matter.
Responsibilities	Identifies who is responsible for adhering to, implementing, and monitoring relevant aspects of the policy or procedure.
Procedures	Outlines how the policy is implemented on a day-to-day basis.
Related Documents	Identifies any other documents that are relevant or important to the policy. While all written material within the organisation is related in one way or another, there will often be particular documents that should be read in conjunction with the policy. Examples may include other policies, Acts of Parliament (or sections of relevant text), the organisation's constitution (or sections of relevant text), etc. Not all policy documents will have Related Documents.
Approval	Certifies that the policy has been through all necessary procedures and is now in force.

Related Documents


- Policy OVL-123-001 Confidentiality

References

<u>Law/Regulation</u>	<u>Citation</u>
HIPAA Privacy Rule	45 C.F.R. Part 160, Part 164 Subparts A, E
HIPAA Security Rule	45 C.F.R. Part 164 Subpart C
HIPAA Breach Notification	45 C.F.R. §§ 164.400–414
HITECH Act	Public Law 111-5 (2009)
FTC Act	15 U.S.C. §§ 41-58
CMIA	Cal. Civ. Code §§ 56-56.37
CCPA/CPRA	Cal. Civ. Code §§ 1798.100–1798.199.100
CalOPPA	Cal. Bus. & Prof. Code §§ 22575–22579
California Data Breach Law	Cal. Civ. Code §§ 1798.29, 1798.82
CAN-SPAM Act	15 U.S.C. §§ 7701–7713

Approval

Approver Signature:

Signed by:

D62E7D911C87429...

 Date: 7/16/2025

Approver Name: **Andrew Mikhail, COO**

Policy Number	ADM-151	Version	002
Drafted By	Cynthia Donate	Effective Date	07/16/2025
Responsible Person	Business Manager	Next Review Date	03/01/2026