



STAUSS PLLC · PRIVACY · AI · CYBER

Presentation to CalPrivacy Board

November 5, 2026

David Stauss

Stauss PLLC — www.staussfirm.com



Notices

NOTICES

Pain Points



Business Pain Points

- Differing legal requirements across states, federal (GLBA and HIPAA), and international laws (e.g., different legal rights, applicability, disclosure requirements)
- Tension between readability and thoroughness
- Should I combine state notices? Should I combine some? Where does my employee privacy policy go?



Consumer Pain Points

- If businesses and their lawyers struggle with these issues, how can consumers understand them?
- Length and legalise of notices make them impenetrable
- Does anyone read them?
- Notice and consent model v. substantive data minimization

NOTICES

Possible Solutions

Revise Regulation 7011 and add a new regulation to:



Allow for the use of short form summaries

- Businesses may provide a short form privacy policy as long as it links to their main privacy policy that provides the full legally-required disclosures



Allow for the use of alternative landing pages and explanatory graphics

- Landing pages where businesses can explain when various documents apply and provide links to consumer rights request forms
- Encourage use graphics and pictures to increase understandability and comprehension

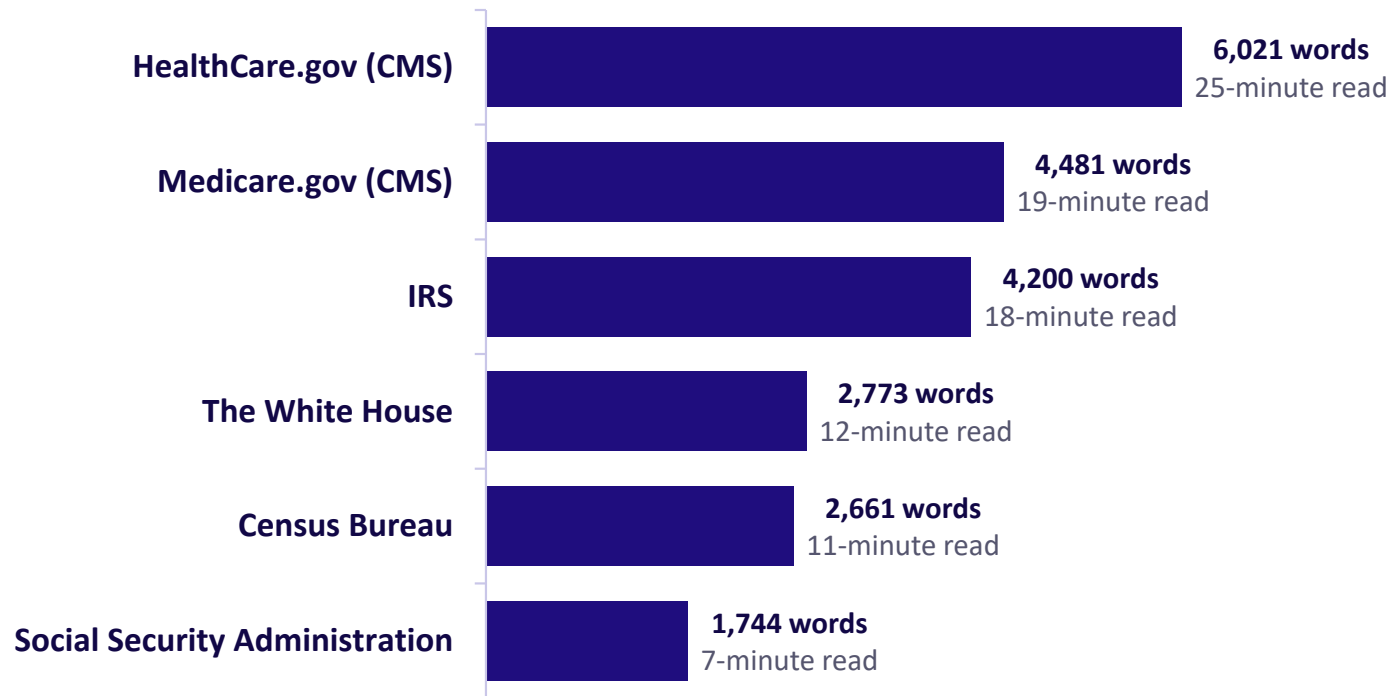


Safe Harbor

- Businesses should be credited with taking additional steps to improve transparency
- Make it clear that businesses will not be faulted for providing these types of pages as long as their long-form disclosures comply with the CCPA

NOTICES

Government Privacy Policies: Length and Read Time



FOR COMPARISON

**Stauss Template
Privacy Policy**

7,000
words

29-minute read

NOTICES

Possible Solutions: 250 Word Summary

HealthCare.gov Privacy Policy: Summary

The Health Insurance Marketplace®, operated by the Centers for Medicare & Medicaid Services (CMS), explains what HealthCare.gov collects, why it collects it, and what it does with it. Information you provide is never sold.

Browsing. The site does not collect your name or Social Security number unless you choose to provide it. It automatically logs details such as your IP address, approximate location, device, browser, pages viewed, and time on page to run the site, measure traffic, and support digital advertising. [Read more.](#)

Applying. Creating an account or applying for coverage collects your name, contact details, and identity-verification information. It is used to determine eligibility, enroll you in a plan, and contact you, and is verified with agencies such as SSA, IRS, and DHS. [Read more.](#)

Cookies and advertising. Session and persistent cookies, web beacons, and third-party tools support analytics, conversion tracking, retargeting, and targeted ads. [Read more.](#)

Your choices. Privacy Settings let you turn off advertising, analytics, and social media tools, and the site honors Do Not Track for ad tracking. You can also ask the call center to stop prerecorded calls. [Read more.](#)

Partners. Help On Demand, enrollment partner websites, and DocuSign appeals follow their own privacy policies. [Read more.](#)

Protection and retention. Records are safeguarded under the Affordable Care Act and the Privacy Act of 1974 and kept only as long as needed. [Read more.](#)

Children. The site is not intended to collect information from children under 13.

Contact. Privacy@cms.hhs.gov or 1-800-318-2596 (TTY 1-855-889-4325).

NOTICES

Possible Solutions: Graphics and Drilldowns

HEALTH INSURANCE MARKETPLACE® · HEALTHCARE.GOV

Your privacy, made simple.

Here is what we collect, why we collect it, and what you can do about it. Tap any box below for a quick answer, then jump to the full policy text.

We never sell your information

You can turn off ad tracking

We honor Do Not Track

You can stop prerecorded calls





04

Your choices

Privacy Settings let you turn off advertising, analytics, and social media tools. We also honor Do Not Track.

[Read the full section →](#)



05

Partner sites and tools

Help On Demand, enrollment partners, and online appeals through DocuSign follow their own privacy policies.

[Read the full section →](#)



06

How we protect it

Your records are safeguarded under the Affordable Care Act and the Privacy Act of 1974.

[Read the full section →](#)



04

Your choices

Privacy Settings let you turn off advertising, analytics, and social media tools. We also honor Do Not Track.

[Read the full section →](#)



05

Partner sites and tools

Help On Demand, enrollment partners, and online appeals through DocuSign follow their own privacy policies.

[Read the full section →](#)



06

How we protect it

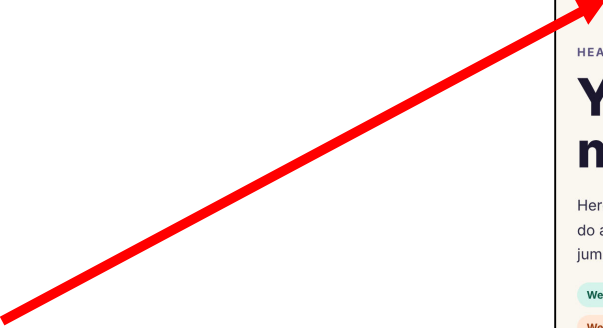
Your records are safeguarded under the Affordable Care Act and the Privacy Act of 1974.

[Read the full section →](#)

NOTICES

Possible Solutions: Graphics and Drilldowns

Adding quick access to Privacy Request Form



Exercise your privacy rights

Use one short online form to ask to see, correct, or delete your personal information, or to ask a privacy question.

[See my data](#) [Correct my data](#) [Delete my data](#) [Ask a question](#)

Open the privacy request form →

Prefer to call? [1-800-318-2596](tel:1-800-318-2596)

HEALTH INSURANCE MARKETPLACE® · HEALTHCARE.GOV

Your privacy, made simple.

Here is what we collect, why we collect it, and what you can do about it. Tap any box below for a quick answer, then jump to the full policy text.

[We never sell your information](#) [You can turn off ad tracking](#)

[We honor Do Not Track](#) [You can stop prerecorded calls](#)

What's in this policy

9 topics. Each box gives the short version; click it to read the full section.

01 What we collect

Visits log basic details like IP address, device, and pages viewed. We get your name and contact details only if you sign up or apply.

[Read the full section →](#)

02 How we use it

To check eligibility, enroll you, and contact you. We verify application details with agencies like SSA, IRS, and DHS. We never sell it.

[Read the full section →](#)

03 Cookies and ads

Cookies, web beacons, and log files help run the site, count visits, and measure and target our ads.

[Read the full section →](#)

04 Your choices

Privacy Settings let you turn off advertising, analytics, and social media tools. We also honor Do Not Track.

05 Partner sites and tools

Help On Demand, enrollment partners, and online appeals through DocuSign follow their own privacy policies.

06 How we protect it

Your records are safeguarded under the Affordable Care Act and the Privacy Act of 1974.

NOTICES

Possible Solutions: Graphics and Drilldowns

Landing page that
organizes various policies
with explanatory text

PRIVACY CENTER

Find the privacy policy that applies to you.

We have different privacy documents for different relationships with us. Tell us who you are below and we'll highlight the ones that apply, or browse all six.

Your Privacy Choices

Submit a privacy request

Cookie settings

Which policy applies to me?

Choose what describes you. More than one policy can apply.

Show all

I use the website or app

I live in California

I'm in the EU or UK

I'm a patient or plan member

I work here or applied for a job

Showing all six privacy documents.

Online Privacy Policy

Applies when: you visit our websites, use our apps, or contact us online. Start here if you're not sure.

Our main policy. It explains what personal information we collect online, how we use and share it, and the choices you have.

- Information we collect and why
- Who we share it with
- Your choices and how to contact us

Updated [DATE] [Read policy →](#)

California Privacy Notice (CCPA)

Applies when: you are a California resident. It adds to the Online Privacy Policy; it doesn't replace it.

Describes the rights California law gives you over your personal information and how to use them.

- Right to know, delete and correct
- Opting out of sale or sharing
- Limiting use of sensitive information

Updated [DATE] [Read notice →](#)

GDPR Privacy Notice

Applies when: you are in the European Economic Area or the United Kingdom, or we process your data there.

Explains our legal basis for using your data, international transfers, and your rights under the GDPR and UK GDPR.

- Access, correction, erasure and portability
- Objecting or withdrawing consent
- Complaining to a data protection authority

Updated [DATE] [Read notice →](#)

HIPAA Notice of Privacy Practices

Applies when: you receive care or health plan coverage from us. It governs your protected health information.

Covers the personal information we handle

Employee & Applicant Privacy Notice

Applies when: you are a current or former employee, contractor, or job applicant.

Covers the personal information we handle

Cookie Statement

Applies when: you visit our websites. It explains the cookies and similar tracking tools we use.

Lists the types of cookies we use, who sets them, and how to manage your preferences.

STAUSS
PRIVACY · AI · CYBER

NOTICES

Possible Solutions: Privacy Nutrition Labels

Privacy Facts	
HealthCare.gov · Health Insurance Marketplace® (CMS)	
Does HealthCare.gov...	Answer
Sell your personal info?	✓ No
Get your name or SSN when you just browse ?	✓ No
Log your IP address , device and pages?	! Yes
Use advertising cookies and web beacons?	! Yes, you can opt out
Share your application with other agencies?	! Yes, to verify it
Use your social media info to target ads?	✓ No
Store cookie data on its own systems?	✓ No

Can you...	Answer
Turn off ad and analytics tools?	✓ Yes, Privacy Settings
Block ad tracking with Do Not Track ?	✓ Yes
Stop prerecorded calls?	✓ Yes, call us
Unsubscribe from emails and texts?	✓ Yes
Use the site with tracking tools off ?	✓ Yes
Apply without the website ?	✓ Yes, by phone

How it's protected
Affordable Care Act · Privacy Act of 1974 · Multi-factor sign-in · Kept only as long as needed

Shared to check your eligibility with
SSA · IRS · DHS · DoD/TRICARE · VHA · State Medicaid and CHIP · Equifax Workforce Solutions

✓ Protects you ! Good to know

Questions? Privacy@cms.hhs.gov · 1-800-318-2596
Last updated 2/27/2025

Does HealthCare.gov...	Answer
Sell your personal info?	✓ No
Get your name or SSN when you just browse ?	✓ No
Log your IP address , device and pages?	! Yes
Use advertising cookies and web beacons?	! Yes, you can opt out
Share your application with other agencies?	! Yes, to verify it
Use your social media info to target ads?	✓ No
Store cookie data on its own systems?	✓ No

Cookie Preferences

This website uses certain cookies and other tracking technologies ("cookies") employed by ██████████ and the companies we work with to automatically collect information about how you access and use our sites and services. We and our advertising and analytics partners may use this information to help us enable and improve site functionality, analyze site usage and assist in our marketing and targeted advertising efforts. Please see our [Privacy Policy](#) and [Supplemental Privacy Notice for U.S. Residents](#) for more on how we collect, use, share, sell, and retain personal information and how to exercise privacy rights. By accessing or continuing to use our site, or by clicking "Agree," you agree to these policies and [Terms of Use](#), which may impact certain important rights. You may opt out of sale and targeted advertising activities or otherwise change your cookie setting by clicking "Manage."

AGREE

MANAGE

This website uses cookies to better understand how visitors use our site, for advertising, and to offer you a more personalized experience.

We share information about your use of our site with analytics, social media, and advertising partners in according with our [Privacy Statement](#) and [California Privacy Notice](#). You can manage this sharing by selecting the "Cookie Settings" link.

[Cookies Settings](#)

X

This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. Select Cookie Settings for more information. By accessing or continuing to use our site, you agree to our [Terms Of Service](#) and our [Privacy Policy](#), which may impact certain important rights.

Cookie Settings

X

Our site uses tracking technologies, like cookies, to offer you a better experience, personalize content and ads, and to analyze and improve our site performance. Use the buttons to the right to provide your online data processing preferences.

Opt out requests for offline Targeted Advertising and Do Not Sell/Share data processing may be submitted [here](#). To learn more about ██████████ data processing, your privacy rights, and how to exercise them, review our [Privacy Policy](#).

Manage Preferences

Reject All

Accept All

Cookie Banner Examples

We use first and third-party cookies and other technologies to provide you with the best experience including to enable site functionality, analytics, personalization and targeted advertising. Select Do Not Sell or Share My Personal Information at the bottom of our page to learn how to opt out of targeted advertising. Review our [Privacy Policy](#) to learn more.

Close



Consumer Requests

Pain Points



Business Pain Points

- **What is a sufficient response?**
 - How much information do I need to provide in response to a request for specific pieces of personal information?
- **Out of box solutions do not exist**
- **Cookie management is a full time / endless job**
- **Consumer use of AI in making requests**
- **Leveraging consumer requests as litigation threats**
 - (If you don't do "X," I will file a lawsuit / report you to a regulator)



Consumer Pain Points

- **Too many links**
 - Your Privacy Choices / Do Not Sell or Share My Personal Information / Privacy Policy / California Privacy Policy / Cookie Preferences / Consumer Health Privacy Policy
- **Rights differ by states**
- **Too much friction to exercise rights**
 - Multiple forms, methods for exercising rights are difficult to find
- **Confusing privacy rights with customer service**
 - E.g., Using right to correct to update mailing address

Pain Points

[Company]

Data Subject Response Manual: Applicable US Data Subject Requests

Policy No.:

Approver:

Owner:

Version: 1

Effective Date:

Next Review Date:

Classification: Confidential

| Data Subject Response Manual: Applicable US Data Subject Requests

Page 1

Table of Contents

1 | SCOPE, METHODS FOR DATA SUBJECT REQUEST SUBMISSION, TYPES OF DATA SUBJECT REQUESTS THAT CAN BE MADE, AND ASSOCIATED DEADLINES.....

2 | IDENTITY VERIFICATION.....

3 | RESPONSES WHEN DENYING REQUESTS BASED ON LACK OF INFORMATION, EXEMPTIONS, OR NO PRIVACY LAW.....

4 | REQUESTS TO KNOW OR ACCESS.....

5 | REQUEST TO DELETE.....

6 | REQUESTS TO CORRECT.....

7 | REQUESTS TO OPT OUT OF SALES, SHARING, OR USE OF PERSONAL INFORMATION FOR TARGETED ADVERTISING.....

8 | REQUESTS TO LIMIT THE USE AND DISCLOSURE OF SENSITIVE PERSONAL INFORMATION.....

9 | REQUESTS TO OPT OUT OF ADMT.....

10 | REQUESTS TO ACCESS ADMT.....

11 | AUTHORIZED AGENTS.....

12 | REQUESTS TO APPEAL.....

13 | WHAT RECORDS TO KEEP AND FOR HOW LONG.....

14 | INSTRUCTIONS TO SERVICE PROVIDERS / CONTRACTORS.....

|

| Data Subject Response Manual: Applicable US Data Subject Requests

Page 2 of 49

CONSUMER REQUESTS

Pain Points: Different Response Timelines



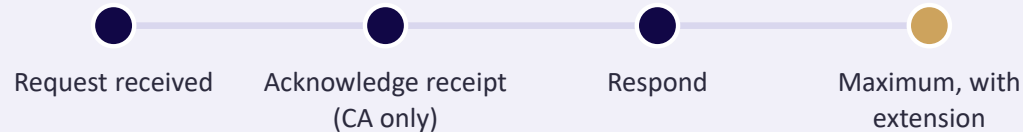
Requests to Know, Access, Access ADMT, Correct, Delete, and Appeal

Day 0

Day 10

Day 45

Day 90



Appeal timelines

45 days: CO, MN, NE, NJ, OR

60 days: CT, DE, IA, IN, KY, LA, MD, MT, NH, OK, RI, TN, VA, VT

No right to appeal: AL, CA, UT



Opt Out of Sales, Sharing, or Targeted Advertising; Limit Use and Disclosure of Sensitive PI; Opt Out of ADMT

Limit and Opt Out of ADMT

- **CA:** 15 business days

Opt-out requests

- **CA:** 15 business days
- **CO:** rule: “without undue delay”; statute: 45 days
- **AL, CT, DE, IN, KY, LA, MD, MN, MT, NE, NH, NJ, OR, OK, RI, TN, TX, UT, VA, VT:** 45 days
- **IA:** 90 days

CONSUMER REQUESTS

Pain Points: Different State Rights

RIGHT	AL	CA	CO	CT	DE	IN	IA	KY	LA	MD	MN	MT	NE	NH	NJ	OK	OR	RI	TN	TX	UT	VT	VA
Know	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Obtain list of third parties to which personal data was disclosed	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗
Data portability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Delete	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Correct inaccuracies	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Not be discriminated against for exercising rights	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Opt-out of sale	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Opt-out of targeted advertising/sharing	✓	✓	✓	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Opt-out of certain types of profiling	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Opt-out of ADMT	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Recognize opt-out signals	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗
Revoke consent	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗
Not process data in discriminatory manner	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Appeal	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓

Possible Solutions



Model Request Webform with a Safe Harbor

Publish a standard webform any business can adopt:

- One entry point for every consumer right
- Plain-language descriptions of each right
- Built-in verification steps and timelines
- **Safe harbor:** businesses that use it are treated as compliant on method and design



Define a Sufficient Response

Provide examples and template responses, especially for requests for specific pieces of personal information



Separate Privacy Rights from Customer Service

Clarify that account and customer service issues (e.g., updating a mailing address) can be redirected without triggering CCPA timelines

GLOBAL

Possible Solutions



Forward Looking

Build structures that can adapt as new laws, technologies, and rights emerge



Beyond Regulation and Enforcement

Education and guidance

Best practices

FAQs

Advisory opinions



Cross-State Collaboration

- Expand mission of State Privacy Consortium to include issuing guidance on areas of commonality
- Leverage stakeholders



European Data Protection Board

- Composed of heads of national data protection authorities from EU and EEA member states.
- Publishes guidelines, recommendations, and best practices to clarify privacy rights and obligations under European law



Thank you

David Stauss – David.Stauss@staussfirm.com

www.staussfirm.com

STAUSS
PRIVACY • AI • CYBER