Clark Hill

Dark Patterns in Healthcare: Navigating Patient Consent, Website Privacy, and Emerging Regulatory Risk

Paul Schmeltzer
Member at Clark Hill
(323) 497-4493
pschmeltzer@clarkhill.com

John Howard
Senior Attorney at Clark Hill
(480) 684-1133
jfhoward@clarkhill.com

August 4, 2026

Agenda

- What dark patterns are—and why healthcare magnifies them
- Patient intake, HIE participation, authorizations, and portal workflows
- Cookie banners, tracking technologies, and digital marketing
- HIPAA, the FTC Act, state privacy laws, and enforcement
- A practical audit and remediation playbook

A dark pattern undermines meaningful choice

WORKING DEFINITION

A design becomes problematic when its effect is to subvert or impair a person's autonomy, decision-making, or choice.

Intent matters less than effect. A well-meaning workflow can still steer patients through defaults, friction, hierarchy, timing, or pressure.

Ask one question

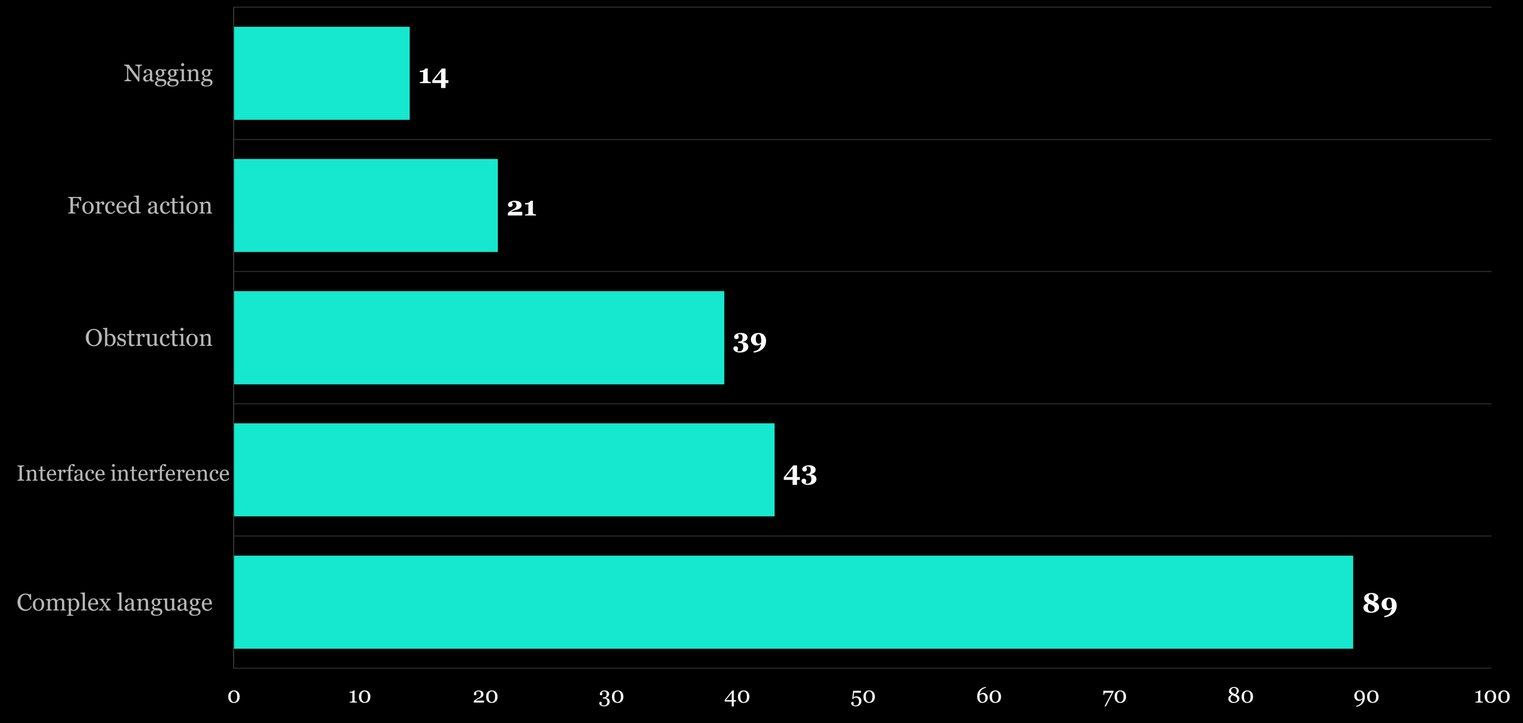
Would a reasonable patient understand the choice—and feel free to say no?

Potential deceptive design patterns are widespread

97%

of 1,010 websites and apps reviewed showed at least one potential deceptive design pattern.

2024 GPEN sweep · 26 privacy authorities



The issue is not whether a workflow has design influence. It is whether that influence undermines a meaningful choice.

Five patterns recur across interfaces

Pattern	What it does	Healthcare example
Complex language	Overwhelms or obscures	Dense authorization buried in intake
Interface interference	Makes one option visually dominant	Large “Continue” / faint “Decline”
Nagging	Repeats prompts until the user gives in	Portal enrollment prompt after every visit
Obstruction	Adds steps to the privacy-protective path	Opt-out requires a form, email, or call
Forced action	Conditions access to evaluation or care on unnecessary data or consent	Non-treatment related forms, consents, acknowledgements, or authorizations, e.g., marketing

A nudge preserves choice but a dark pattern distorts it

HELPFUL CHOICE ARCHITECTURE

Encourages a beneficial action

States the purpose plainly
Preserves a realistic “no”
Uses neutral visual treatment
Makes reversal easy
Avoids unrelated data collection

MANIPULATIVE CHOICE ARCHITECTURE

Steers toward the organization’s preferred outcome

Making an optional choice seem required
Exaggerates consequences of declining
Makes “yes” faster or more prominent
Uses defaults, repetition, or urgency
Couples care with secondary purposes

Healthcare amplifies small design pressures

Patients often decide under conditions that reduce time, attention, and willingness to challenge the workflow.

PAIN	Attention is divided.
ANXIETY	The stakes feel immediate.
TIME PRESSURE	Paperwork delays care.
TRUST	Provider requests carry weight.
INFORMATION GAP	Patients do not know what is optional.

Design risk rises when refusal feels like friction in the path to care.

The risk follows the decision—not the screen

The same autonomy problem can appear in digital, paper, and staff-mediated workflows.

Review the entire journey: what the patient sees, what happens by default, what staff say, when choices are asked to be made, and what the system transmits.

One “I accept” button can erase a stated opt-out

REPORTED PATIENT-REGISTRATION FLOW

The notice said the patient could opt out of HIE sharing.

1	**Notice referenced an opt-out form**	No link was provided
2	**Alternative was to accept now**	Then email later to begin opting out
3	**Signature screen presented one path**	“I accept” → sign → Continue

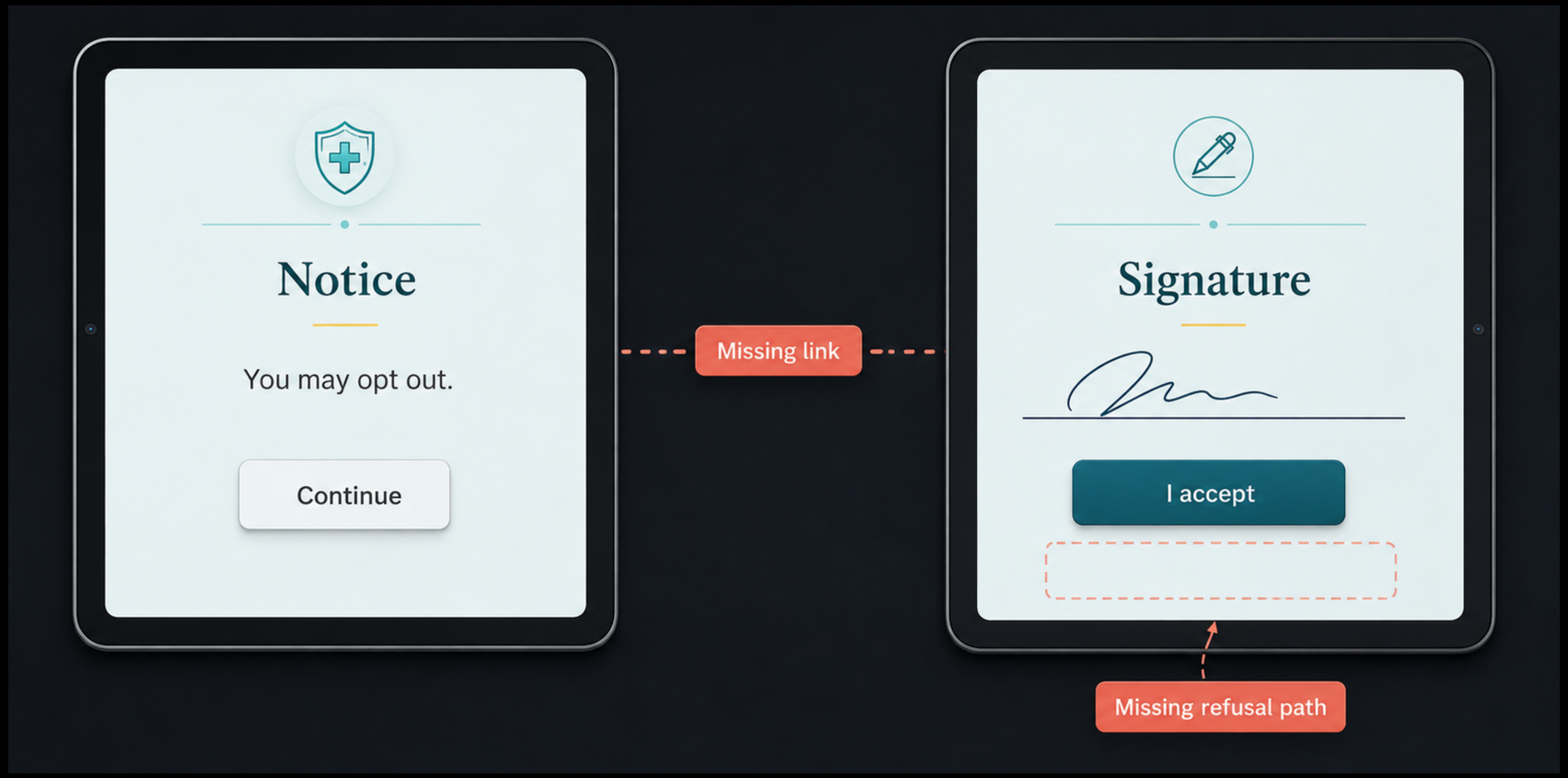
WHY THIS MATTERS

The text described a choice the interface did not operationalize.

The privacy-protective path required more effort and delay.

The need for care increased pressure to proceed.

The record may capture consent without capturing meaningful choice.


Notice
You may opt out.
Continue
Missing link
Signature
I accept
Missing refusal path

Review the text, placement, and process

TEXT	**What does the disclosure say?**	Accurate scope · plain language · optionality
PLACEMENT	**How is the choice visually framed?**	Prominence · grouping · timing · button hierarchy
PROCESS	**What must the patient actually do?**	Defaults · steps · withdrawal · staff script · system behavior

Legal sufficiency at only one layer does not cure a defect at the others.

Intake workflows contain recurring risk signals

Decision	Risk signal	Safer design
Notice of Privacy Practices	Required acknowledgment before notice is available	Show or deliver notice before acknowledgment
Marketing authorization	Embedded in treatment or financial forms	Separate, optional authorization
Patient portal	Enrollment selected by default	Neutral, unselected choice
HIE participation	Opt-out link absent or deferred	Actionable opt-out at the decision point
Research / data use	Repeated prompts after decline	Respect refusal; define a limited re-ask rule
Financial / autopay	Secondary terms placed above care signature	Separate assent and explain consequences

HIPAA is necessary—but not the whole analysis

HIPAA DIRECTLY ADDRESSES

Limits on uses and disclosures of PHI
Core elements and form of valid authorizations
Marketing authorizations in specified circumstances
Notice-of-privacy-practices obligations
Tracking disclosures when the information is PHI

HIPAA DOES NOT EXPRESSLY SUPPLY

A general statutory definition of “dark pattern”
A universal visual-symmetry rule for all patient choices
Entity-wide protection for every health-related data flow
A substitute for FTC or state privacy analysis
Permission created merely by a website notice or banner

The design question often enters through validity, deception, transparency, meaningful choice, and the actual data flow.

Not every signature means the same thing

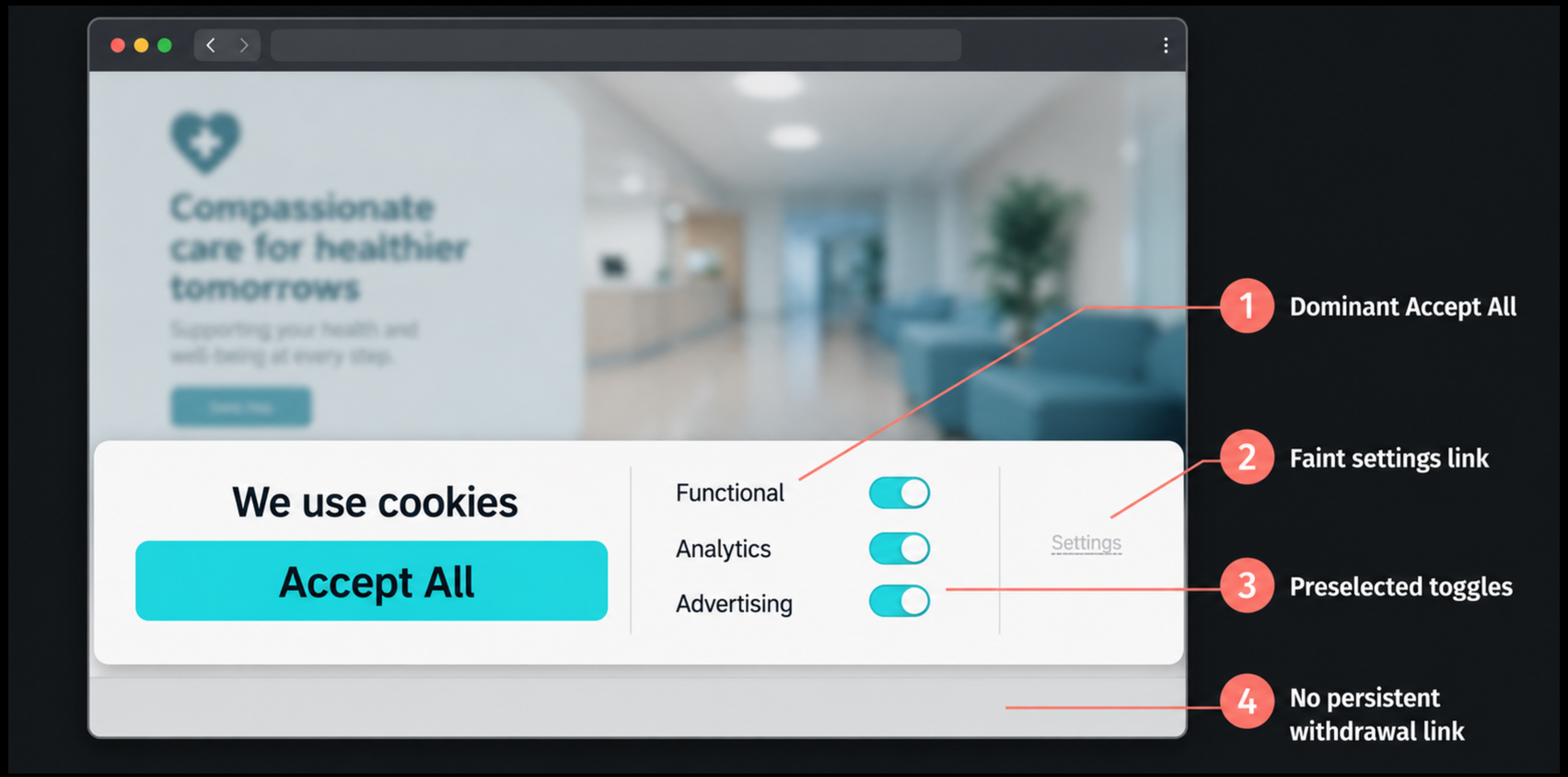
Patient action	Typical purpose	Design implication
Acknowledgment	Confirms receipt of a notice	Do not convert receipt into permission
Consent to treatment	Authorizes care	Do not bundle unrelated secondary uses
HIPAA authorization	Permits specified uses/disclosures	Keep specific, voluntary, and revocable
Privacy opt-in	Permits data processing under another law	Use affirmative, unambiguous choice
Preference	Selects a communication or service setting	Honor defaults, changes, and withdrawal

Start by classifying the legal act. Then design the choice to match it.

Multiple laws now police the architecture of consent

Authority	Design / consent hook	Healthcare relevance
HIPAA	Valid authorization; notice; permitted PHI disclosure	Covered entities, BAs, and PHI—not every health-data flow
FTC Act + HBNR	Unfair/deceptive practices; affirmative express consent; breach notice	Health apps and other non-HIPAA actors; privacy promises and sharing
California CCPA / CPRA	Dark-pattern agreement is not consent; symmetry and clear language	PHI/medical-information exemptions are not a blanket entity exemption
Washington My Health My Data	Opt-in, voluntary, unambiguous consent; deceptive designs barred	Broad consumer health data; private action through state CPA
Colorado Privacy Act	Consent excludes agreement obtained through dark patterns	Sensitive-data processing outside applicable exemptions
State UDAP laws	Unfair or deceptive presentation and omissions	Can reach forms, scripts, portals, advertising, and representations

Current through July 28, 2026 · applicability and exemptions require fact-specific analysis.


Compassionate care for healthier tomorrows
We use cookies
Accept All
Functional
Analytics
Advertising
Settings
1 Dominant Accept All
2 Faint settings link
3 Preselected toggles
4 No persistent withdrawal link

Cookie banners fail in predictable ways

LOADS FIRST

Analytics or advertising tags fire before the user's choice.

FALSE CHOICE

"Accept All" is prominent; refusal is buried behind settings.

PRESELECTION

Optional cookies start on or are marked active by default.

ASYMMETRY

Opt-out takes more clicks than opt-in or re-consent.

CONFUSING LABELS

Categories and purposes do not match actual vendor behavior.

NO WITHDRAWAL

The banner disappears without a persistent privacy-choice link.

A compliant-looking banner cannot cure tags that already transmitted data.

Symmetry is now an enforcement metric

COOKIE TOOL

1 click

to “Allow All” after opting out

2 steps

toggle off + “Confirm My Choices”

$632,500

CPPA administrative fine across alleged CCPA violations

Excessive information for opt-out and limit requests
Unequal privacy choices
Authorized-agent barriers
Ad-tech contracting deficiencies

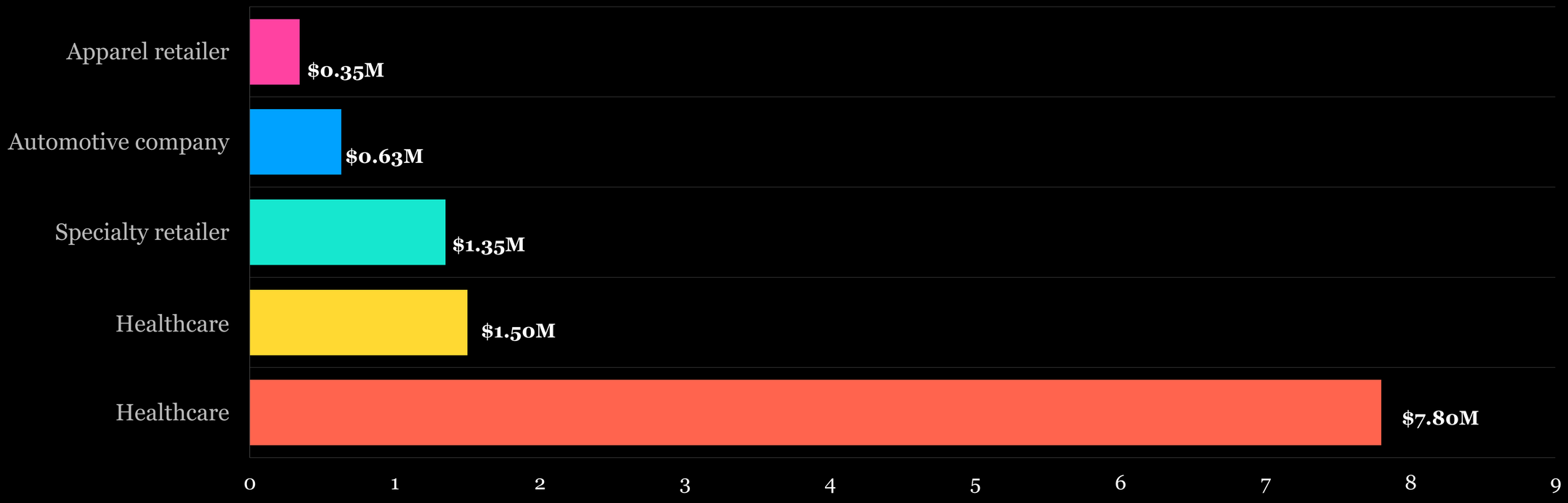
The order required a simpler process and UX review—not just revised legal text.

Privacy friction is generating real penalties

Matter	Fine	Alleged operational failure	Lesson
Automotive Company Mar. 2025	$632,500	Excessive verification; asymmetric choices; agent barriers	Count steps and data fields
Apparel Retailer May 2025	$345,178	Opt-out portal failed for 40 days; excessive data and verification	Test the tool continuously
Specialty Retailer Sept. 2025	$1.35M	Ineffective opt-out, including GPC; notice and contract failures	Inventory tags and honor signals

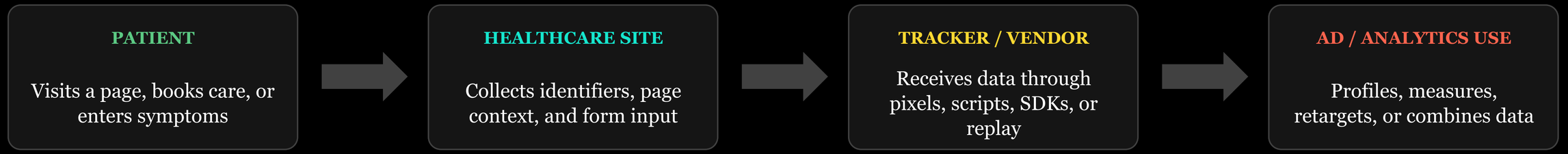
Enforcement is moving from policy wording to whether the privacy mechanism actually works.

Health-data enforcement carries the largest price tags



Representative public payments/fines; matters involve different laws and allegations and are shown for scale—not as a single dark-pattern category.

Tracking can turn a click into a disclosure that creates legal liability



The patient may see only a page. The organization must evaluate every transmission behind it.

A privacy notice alone does not authorize an otherwise impermissible PHI disclosure.

Context determines whether tracking data is PHI

Context	OCR guidance	Compliance focus
Authenticated portal	Tracking technologies generally have access to PHI	Remove, configure, or ensure permitted use + BAA
Appointment / registration page	Identifiers or reasons for care can be PHI	Map every field and transmitted parameter
Symptom or health-analysis tool	Entered health information can be PHI	Prevent unauthorized third-party collection
General hours / job page	A visit alone generally is not PHI	Still assess other privacy laws and actual payload
Non-HIPAA health app	HIPAA may not apply	FTC Act, HBNR, and state health-data laws may

Do not classify by URL alone. Inspect the user's action and the transmitted data.

A consent platform does not outsource accountability

“We installed a banner” is not a compliance conclusion.

LEGAL	Define purposes, legal basis, exemptions, and required consent.
TECHNICAL	Inventory tags; test firing order, payloads, GPC, and withdrawal.
UX	Measure clarity, symmetry, steps, defaults, and prominence.
VENDOR	Configure the platform; validate contracts and downstream use.
OPERATIONS	Assign ownership, monitoring, change control, and evidence.

OWNER

One accountable function must connect all five disciplines.

Audit the journey, not just the document

01 **INVENTORY**

List every patient-facing choice and associated data flow.

02 **CLASSIFY**

Identify acknowledgment, consent, authorization, opt-out, or preference.

03 **CAPTURE**

Record screens, forms, scripts, clicks, defaults, and network calls.

04 **RED-TEAM**

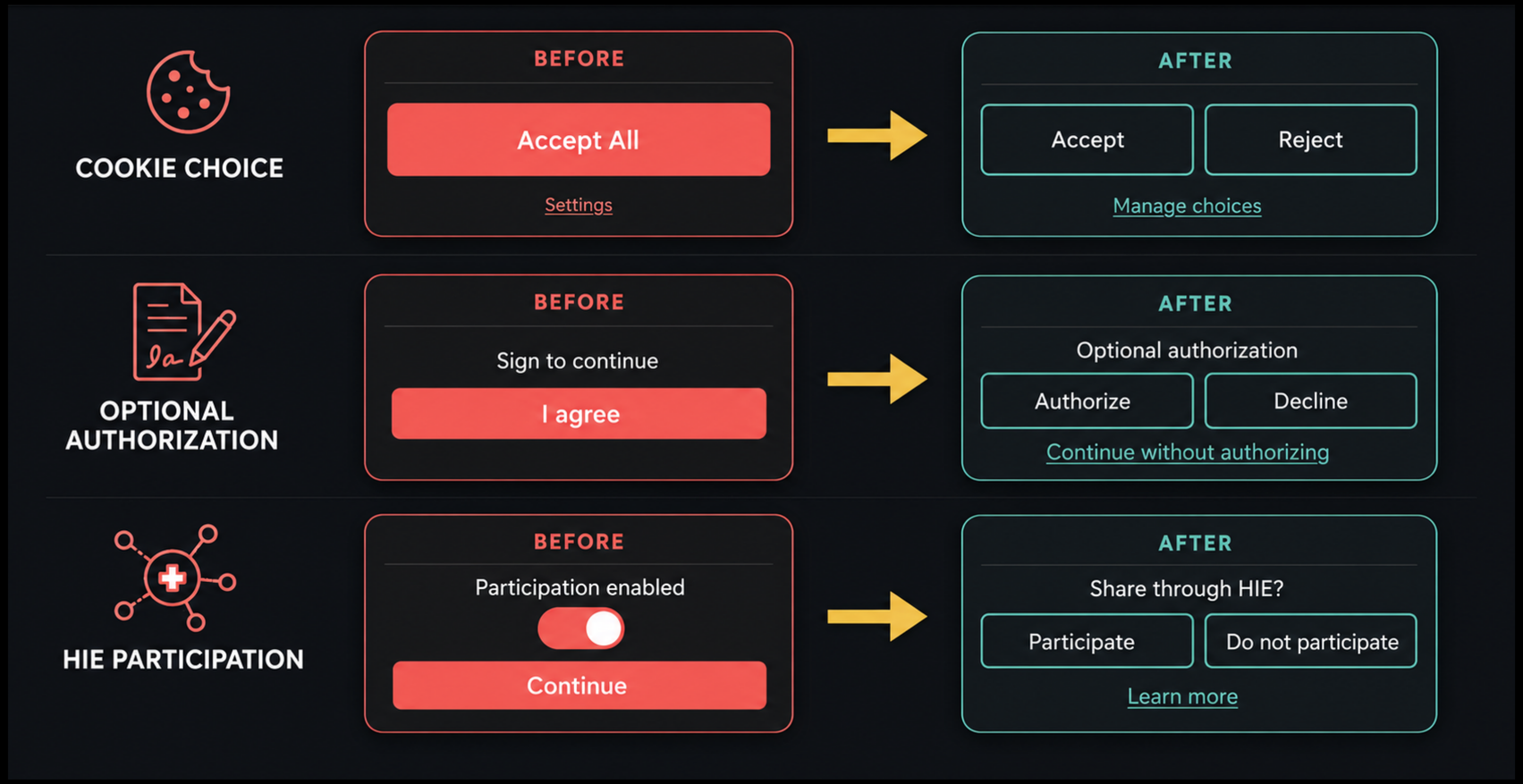
Try to refuse, withdraw, use an authorized agent, and complete the task on mobile.

05 **REMEDIATE**

Shorten, separate, equalize, minimize, and fix technical sequencing.

06 **EVIDENCE**

Retain approvals, test results, versions, owners, and monitoring records.


COOKIE CHOICE
BEFORE
Accept All
Settings
AFTER
Accept
Reject
Manage choices
OPTIONAL AUTHORIZATION
BEFORE
Sign to continue
I agree
AFTER
Optional authorization
Authorize
Decline
Continue without authorizing
HIE PARTICIPATION
BEFORE
Participation enabled
Continue
AFTER
Share through HIE?
Participate
Do not participate
Learn more

Score each choice for defensibility

Test	Green	Yellow	Red
Clarity	Plain; purpose-specific	Some jargon or cross-reference	Ambiguous or hidden
Symmetry	Comparable steps and prominence	Minor friction difference	“Yes” materially easier
Necessity	Only data needed	Extra optional fields	Unnecessary data required
Reversibility	Easy withdrawal	Manual follow-up	No practical reversal
Timing	Choice before processing	Unclear sequencing	Tags / sharing occur first
Evidence	Tested and documented	Owner known; tests incomplete	No owner or audit trail

Any red score warrants remediation or a documented legal and operational rationale.

Small design changes can materially reduce risk

	HIGHER-RISK PATTERN		MORE DEFENSIBLE ALTERNATIVE
COOKIE CHOICE	Accept All | Manage Settings	→	Accept All | Decline All
OPTIONAL AUTHORIZATION	Embedded above treatment signature	→	Separate form; explicit “declining will not affect care”
HIE PARTICIPATION	Accept now; email later to opt out	→	Opt in | Opt out at the same step

The goal is not visual neutrality in the abstract. It is a clear, voluntary, and operationally real choice.

Design the choice you would want to defend

CLEAR	Patients can understand the purpose and consequence.
SEPARATE	Optional permissions are not bundled with care.
SYMMETRICAL	The privacy-protective path is not harder.
TRUE IN PRACTICE	**The interface, staff script, and data flow match.**
PROVABLE	The organization can show testing, ownership, and monitoring.

If a regulator replayed the patient journey, what would the design communicate?

Thank You

Legal Disclaimer
The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill