New Class Action Targets Healthcare AI Recordings: 6 Steps All Businesses Should Consider to Limit Exposure

Insights
12.09.25

A newly filed class action in San Diego highlights a key risk for any business deploying AI tools that listen, record, or summarize customer or patient conversations. On November 26, Sharp HealthCare was hit with a sweeping privacy lawsuit alleging it secretly used an AI-powered "ambient clinical documentation" tool to record doctor–patient conversations without proper consent. And while healthcare may be the target of this lawsuit, any consumer-facing business using AI voice tools, quality-assurance recording, or conversation-analysis engines should take note. This Insight covers what happened, why plaintiffs view these cases as high-value opportunities, and six steps your business can take now before your own AI tools become tomorrow's class-action headline.

Lawsuit Highlights Key Risks Faced with AI Recording Tools

According to the complaint, Sharp deployed an AI vendor in April 2025 to automatically record clinical encounters on clinicians' devices and generate draft notes for the electronic health record. The lawsuit alleges:

- **Sharp** did not obtain **all-party consent** before recording confidential doctor-patient conversations as required under California's strict wiretapping law (CIPA). The plaintiffs claim ambient AI documentation amounts to electronic eavesdropping, even if the vendor never "listens" in the human sense. Simply capturing audio and sending it outside the organization (even for transcription) is enough for liability, they claim.
- **Medical information** (symptoms, diagnoses, medications, treatment plans, personal identifiers) was transmitted to the vendor's cloud system where vendor personnel could allegedly access the data, violating California's Confidentiality of Medical Information Act (CMIA).
- **False documentation** appeared in patient charts stating that patients "were advised" and "consented" to the AI recording even when they had not. The plaintiffs fault Sharp for not using encounter-specific verbal consent, pre-visit notices, on-screen or auditory indicators that recording was active, or written authorizations.
- Sharp allegedly told the patient that the vendor retained audio for ~30 days and **could not immediately delete upon request**.

The complaint seeks statutory penalties, punitive damages, injunctive relief, and full correction of allegedly inaccurate medical records for a class that may exceed 100,000 patients.

> ⚠ It's important to note that these are simply allegations at this very early stage of the litigation, and we only have one side of the story. Sharp hasn't yet had an opportunity to respond. Regardless of whether these allegations are proven, however, the lawsuit provides a perfect opportunity for businesses in healthcare and beyond to review their practices.

Why This Case Matters Beyond Healthcare

There are several reasons why businesses across all industries need to pay attention to this litigation.

AI Recording Tools Create Potential CIPA Exposure

CIPA is one of the most plaintiff-friendly wiretapping statutes in the country, as you can track on FP's **Digital Wiretapping Litigation Map**. It may provide $5,000 per violation, per call, per recording. That math is why plaintiffs' firms continue to file cases against retailers, banks, hospitality brands, and service providers using call-center recording, chatbot summarization, or "voice intelligence" platforms.

AI Vendors Are Advertising Their Customer Wins

As more AI vendors publicize major client partnerships ("Over 1,000 providers use our ambient AI tools"), plaintiffs' firms see this as an easy roadmap. Plaintiffs use the existence of public customer lists as prebuilt class definitions.

The Theories Apply Across Industries

The claims brought up in this case (wiretapping, improper disclosure to third-party AI vendors, false or misleading consent statements, retention failures, lack of opt-outs, etc.) are the exact theories we see emerging in other industries. These include:

- Retail customer-service recordings
- Any customer intake calls
- Financial-services call analytics
- Hospitality and travel agencies' chat/voice systems
- Any company piloting "AI-powered note-taking"

6 Practical Steps Businesses Can Take Now

Here are six practical steps you can consider deploying today in order to minimize the chances of getting hit with a class action lawsuit tomorrow.

1. Audit Any Technology That Captures or Transmits Voice or Text During Customer Interactions

The most common areas we now see include AI note-taking tools, whisper/API transcription tools, "agent assist" or "quality assurance analytics," and virtual agents that record audio or text inputs. Map where audio goes, who receives it, and how long vendors retain it.

2. Implement Clear Consent Protocols

Your business should consider:

- **Pre-interaction notice** (on websites, intake forms, appointment reminders, IVR prompts)
- **Real-time consent** at the start of the encounter
- **Visible/audible indicators** if recording is active
- **Separate written authorization** if health or financial information is involved in California

3. Rewrite Vendor Contracts Now

Review whether contracts with AI transcription or analytics vendors include:

- Customer-controlled retention and deletion
- No secondary use of data (training, QA, model development) without explicit consent
- Immutable logging of access and deletion
- Requirements for certificates of destruction
- Prohibition on vendor personnel accessing identifiable recordings unless specifically authorized

4. Ensure Vendors Don't Take Liberties

Don't consent to your vendor using your name as their customer, or publishing a case study press release about your company's use of their AI tool, without consulting your AI legal counsel about the implications. It's common for companies to bring their Marketing and PR teams into the fold when these opportunities arise, but less common for companies to ask the Legal Department to weigh in – until the inevitable lawsuit appears. Other times, the manager responsible for the vendor relationship approves the vendor's request to list the company as a customer on their website or to provide a testimonial without gaining Legal's approval. Make sure this doesn't happen at your organization.

5. Disable Any Default "Consent" Auto-Population

If your AI system inserts boilerplate such as "customer consented," make sure it is turned off. You should aim to require manual confirmation, audit trails, and a separation between consent capture and documentation fields.

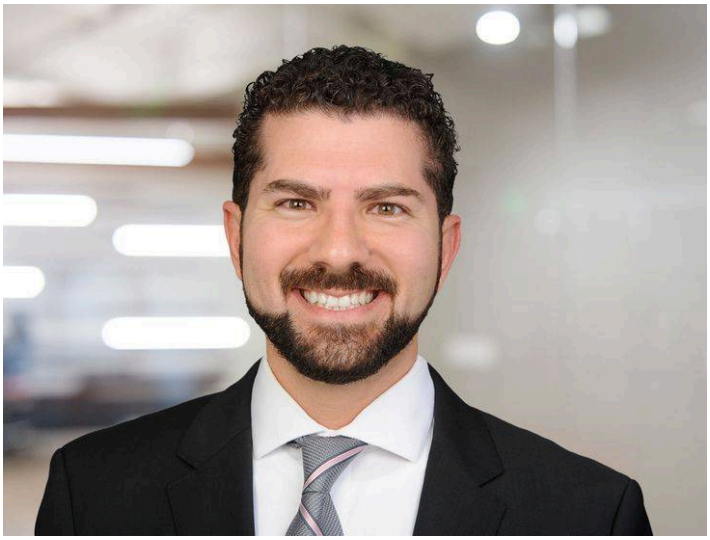
6. Build a Fast, Verifiable Deletion Workflow

Courts increasingly view deletion-on-demand as part of basic privacy hygiene, especially in California. For this reason, businesses should be able to immediately halt processing, submit a verified deletion request to the vendor, and provide the customer with written confirmation of deletion.

Conclusion

We will continue to monitor this type of litigation and related developments and provide the most up-to-date information directly to your inbox, so make sure you are subscribed to Fisher Phillips' Insight System – and check out FP's AI Litigation Tracker here. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI, Data, and Analytics Practice Group, our Privacy and Cyber Practice Group or Consumer Privacy Team, or our Healthcare Industry Team.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Danielle Kays
Partner
312.260.4751
Email

Service Focus

Privacy and Cyber

Litigation and Trials

Consumer Privacy Team

Industry Focus

Healthcare

Trending

U.S. Privacy Hub