Surveillance by Proxy: How UnitedHealthcare Evaded HIPAA Using Local Law Enforcement

“The right to be let alone—the most comprehensive of rights, and the right most valued by civilized men.”
—Justice Louis Brandeis, *Olmstead v. United States*, 277 U.S. 438 (1928)

By Samara Dorn
Transgender plaintiff. Litigant. Survivor. Future precedent.

Sep 12, 2025

Abstract
In January 2025, UnitedHealthcare of Colorado transmitted a transgender patient’s protected health information—including audio recordings, psychiatric medication lists, and gender-affirming care history—to local law enforcement without legal process, justification, or consent. This commentary argues that the disclosure was not merely a HIPAA violation, but an intentional act of political and administrative erasure rooted in systemic transphobia. Drawing from statutory analysis (45 C.F.R. § 164.512(j)), documented metadata, and internal admissions by UnitedHealthcare personnel, the author positions the breach as a constitutional and civil-rights crisis with implications far beyond one case. By situating the event within the broader context of Project 2025 and post-2024 anti-trans rhetoric, the piece warns of a precedent whereby metadata, AI escalation systems, and “wellness” surveillance can be weaponized to digitally erase marginalized people under the guise of healthcare compliance.

A newly added section examines how a late-July 2025 local news article—which did not name the patient—publicly replicated the insurer-to-police escalation through sequencing and omission. Using a defamation-safe, structural-forensics approach (headline/subhead gravity, quote adjacency, timeline fusion, and mosaic re-identification risk), the analysis frames these dynamics as media echo, not collusion, and proposes newsroom process remedies. These same presentation mechanics now form part of the factual basis of the Plaintiff’s pending defamation and defamation by implication (gist). action, Mesa County District Court, Case No. 2025-CV-61, and intersect with her broader HIPAA, privacy, and civil-rights action against UnitedHealthcare and affiliates, Mesa County District Court, Case No. 2025-CV-73. The commentary concludes with a legal and moral call to action: if left unchallenged, such practices normalize a quiet form of systemic erasure—where protest is reframed as threat and care becomes the cover for disappearance.

I. THE QUOTES THAT LIT THE MATCH

> "We will continue to guard against unnecessary care." —Andrew Witty, former CEO of UnitedHealth Group (statement during tenure)

> "On the first day, we will revoke Joe Biden’s cruel policies on transgender treatments. We will protect our children—and stop taxpayer funding for transgender procedures and drugs." —Donald J. Trump, October 16, 2024 (Townhall Pledge)

These statements were not isolated outbursts. They were signals. Coordinated, high-level declarations that transgender identity is incompatible with public life, that our care is fraudulent, and that our existence is up for policy debate.

UnitedHealthcare's quote wasn't just poor phrasing. It was a corporate echo of the Trump-Vance platform. A dog whistle rebranded as healthcare governance. It declared that trans people's care is "unnecessary," and by extension, so are we.

The convergence of this rhetoric with UnitedHealthcare's internal behavior cannot be dismissed as coincidence. It reflects the institutionalization of bias: political hate speech normalized and operationalized by a Fortune 5 insurer.

Days later, that signal became my reality.

II. WHAT THEY DID TO ME

On January 15, 2025, UnitedHealthcare of Colorado, Inc. transmitted five audio recordings, my protected health information (PHI), surgical history, psychiatric medication list, and a narrative framing me as a potential threat to public safety, to the Grand Junction Police Department. There was:

- No warrant
- No subpoena
- No legal process
- No documented emergency

There was only metadata, subjective impressions, and a political climate primed to treat transgender advocacy as destabilizing.

They didn't notify me. They didn't verify my clinical risk. They didn't redact or anonymize anything. They offered no justification other than internal speculation.

They sent my entire identity to law enforcement—in the form of recordings, diagnoses, and stigmatizing interpretation—not because I posed a clinical threat, but because I challenged their denial of care.

The sequence matters. First, they attempted an escalation through federal channels. When that did not result in action, they pivoted to local law enforcement. That is not concern; that is **administrative escalation**—a second bite at the apple after a first attempt failed. No warrant. No subpoena. No documented emergency.

This wasn't a medical response. It was a covert reclassification of a healthcare complaint into a law enforcement matter. A trans woman, denied estrogen after surgery, had her privacy weaponized because she dared to use political language—"Deny. Defend. Depose."—in protest.

It is impossible to separate this conduct from the political environment that encouraged it. UnitedHealthcare moved with confidence—in a country where the President and leading Senators had already labeled people like me as threats to be managed, not citizens to be protected.

Surveillance becomes isolation.
Isolation becomes disappearance.
Disappearance becomes death.

LEGAL CONTRAST: Why This Was Unlawful Under HIPAA

HIPAA allows for disclosures without patient consent only in rare cases. The relevant law—45 C.F.R. § 164.512(j)—requires:

- A good faith belief that disclosure is necessary to prevent or lessen a "serious and imminent threat" to the health or safety of a person or the public, and
- That the disclosure is made to someone reasonably able to prevent or lessen that threat.

In this case:

- No imminent threat was documented.
- More than a month had passed since the last call.
- Police inactivated the referral within 72 hours.
- No charges were filed.

Even UnitedHealthcare's own internal communications acknowledged probable illegality:

"We probably weren't allowed to send that... but it's done." —UHC staff

Thus, this disclosure violated not only the letter of HIPAA, but also its core intent: to protect vulnerable patients from institutional misuse of sensitive health data.

III. THE RETRIBUTIVE MACHINE

Why did they do it? Because I DARED say the phrase:

"Deny. Defend. Depose."

Three words. Legal critique. Insurance-lit shorthand. Activist vernacular. Words you hear in depositions, rallies, and accountability hearings. I used them as a call to action—a demand for institutional redress after being denied medically necessary care.

UnitedHealthcare seized on those words—not because they believed I was dangerous, but because I had become inconvenient. Context was ignored; tone exaggerated; impact weaponized.

I said those three words in the immediate aftermath of widely reported news about a fatal shooting of a health-care executive. Some coverage and online discourse associated that phrase with the event. I knew that—and I said it anyway. **Not as a threat. Not as solidarity.** As a legal critique. As political defiance at a moment when trans speech was being framed as destabilizing. *This is contextual media association—not an admission of linkage or intent.* That association in the news cycle became a pretext: my advocacy was repackaged as complicity because it served a fear-driven narrative of deviance and danger.

Instead of routing my complaint through a grievance process or a clinical ombuds, the matter was escalated through security/legal channels. They didn't want resolution. They wanted removal. By reframing protected speech as a "safety" signal, advocacy became alleged instability; grievance became "risk."

This was not a good-faith error. It was an institutional escalation by a Fortune 5 company seeking to silence dissent through administrative criminalization.

The New COINTELPRO (with dashboards)

Surveillance evolves with its tools:

- voice recordings instead of wiretaps
- HIPAA codes instead of informants
- AI risk scores instead of FBI memos

This was not protection. It was **preemption**. A corporation flagged a trans woman's advocacy as dangerous—then **handed it to the state**. No warrant. No subpoena. No imminent threat. *(Police inactivated the referral within days; no charges were filed.)* Yet the escalation file lived on.

The result: **compliance theater** where a patient's protest is mislabeled as volatility, and "safety" becomes the script for disappearance.

IV. THE ADMINISTRATIVE BLUEPRINT

> "The most effective way to destroy people is to deny and obliterate their own understanding of their history." —George Orwell (warning, not endorsement)

What UnitedHealthcare did isn't new. It is the modern form of elimination through information:

- The Nazis tracked Jews, Roma, homosexuals, and disabled people with exhaustive files
- The Stasi profiled dissidents and LGBTQ+ people by surveilling calls, language, and behavior
- Project 2025 proposes a U.S. version: over 300 data points per citizen, tagged for compliance

Metadata becomes ideology. Behavior becomes risk. Identity becomes a pretext for escalation.

In 2025, they don't need camps. They need cover letters. They need voice logs. They need a reason to classify you.

I was classified.

UnitedHealthcare did not simply just breach my privacy. They erased my right to exist without fear of classification. They transformed a patient grievance into a police matter. They built a profile of me as unstable, agitated, and unfit—not because I was dangerous, but because I was inconvenient.

That is eliminationist logic. It is the same logic that underpinned eugenics programs, forced sterilizations, and psychiatric incarceration of gender nonconforming people for over a century. What begins as a so-called risk assessment becomes a campaign of erasure, not through violence at first, but through administrative targeting. It is the medicalization of rejection. It is an insurer deciding which identities are worth protecting—and which are worth purging from the system.

As legal scholar Danielle Citron writes, "Intimate privacy is not just about secrets—it's about survival. It's the boundary that keeps the powerful from swallowing the powerless." UnitedHealthcare crossed that boundary with full institutional force.

In the early 20th century, this logic took the form of asylums and surgical interventions, targeting women, queers, and the neurodivergent for "moral treatment." In the 21st century, it takes the form of escalation dashboards, metadata flags, and coded referrals to law enforcement. It wears a badge of policy. It hides behind compliance. But its objective is the same: remove the deviant, silence the resistant, disappear the inconvenient.

> "We do not say that every being with a human face is human." —Joseph Goebbels, 1938

This is what that sentiment looks like in 2025:

> "We probably weren't allowed to send that... but it's done." —UHC staff

What starts as concern becomes code. What starts as escalation becomes exile.

They didn't just treat me as a disruption—they reclassified me as a threat. They took the voice of a patient pleading for care and reframed it as evidence of instability. They sent recordings not to a grievance board or to clinical review—but to armed agents of the state. They knew the risk. They knew the law. They sent it anyway.

This is not neutral error. This is not "overcommunication." This is the intentional creation of a profile—a case file—not for healing, but for harm.

When corporate actors decide that distress is synonymous with danger, every cry for help becomes self-incrimination. That is the chilling effect. That is the invisible wall that now divides trans people from care, from justice, from survival.

Erasure no longer looks like sterilization wards or lobotomy units. It looks like risk flags. It looks like the absence of follow-up. It looks like your name in a law enforcement system before you ever speak to a doctor.

It looks like this:

"We probably weren't allowed to send that... but it's done."

And by the time you find out, the damage is already inflicted. The narrative is already shaped.

Because what they sent wasn't just information. It was an invitation to surveil. To discredit. To disappear.

That is elimination by design. Bureaucratic disappearance masked as administrative vigilance.

And it begins with a breach—but ends with a blacklist.

V. DIGITAL LYNCHING IS STILL LYNCHING

The lynching no longer requires a mob.
It requires a metadata file, a prejudiced interpretation, and a convenient narrative.

The violence has changed format. It doesn't wear hoods; it wears **badges that read "compliance" and "security."** It happens across dashboards, escalation meetings, and email threads titled "Member Distress." Not in back alleys—**in backend systems.** Clean. Clerical. Consequential.

They didn't pull a trigger. They **pulled the digital equivalent**: handing me to police in Colorado with PHI-tinged context, after weeks of silence, and **after the crisis had passed.** I wasn't protected. I was **flagged, framed, and nearly disappeared.** Police found **no ongoing threat** and closed the referral—yet the aura of danger persisted.

This isn't theoretical. It happened.
And when it happens at scale, it becomes **systemic erasure**—what I have elsewhere described (as opinion) as "procedural genocide," meaning the cumulative destruction of a person's social and civic standing through files, flags, and process. The point is not hyperbole; it's **mechanism**:

- build a file
- misread distress as danger

- elevate reputation risk over clinical care
- convert a grievance into a permanent record

Like COINTELPRO with HIPAA metadata.
Like “predictive policing” wrapped in a member-escalation dashboard.
They don’t need to outlaw us. **They only need to flag us.**

Classification precedes punishment. **Every flag hardens into a story.** And in small markets, a story doesn’t have to print a name to name you.

VI. THE DANGEROUS PRECEDENT IF WE LET THIS STAND

“What is done cannot be undone, but one can prevent it happening again.” —Anne Frank

If this conduct is tolerated, here’s what follows:

- **Law-enforcement referrals of distressed patients**—not for crime, but for **speech and tone**.
- **Risk scores with identity hooks** (gender identity, disability, neurodivergence) quietly added to health records and shared across networks.
- **Police paperwork as compliance theater,** where challenging a denial becomes a public-safety storyline.
- **Cross-agency fusion justified by “wellness,”** eroding Fourth and Fourteenth Amendment boundaries in the gray zones of “safety.”
- **AI escalation models** that train on protest as instability and anger as “imminent threat.”
- **A chilling effect** so severe that patients stop calling, appealing, or seeking care to avoid being flagged.

Add the modern amplifier:

- **Media echo of risk metadata.** Once a PHI-adjacent escalation appears in print via fused timelines and de-contextualized quotes, the **public gist** hardens—even where police found **no ongoing threat** and closed the matter.

This isn’t futurism. It’s the prototype we are already living.

What is at stake legally:
A Fortune 5 company transmitted PHI to police **without legal process**, recast political/therapeutic speech as threat, and operated **outside** HIPAA’s emergency framework. If subjective impressions and dashboards can override consent and statutory thresholds, privacy law exists only as **decoration**.

VII. THE COMING INFRASTRUCTURE OF DIGITAL ERASURE

This isn't a one-off. It's a prototype—an operational pilot for an identity-driven surveillance apparatus.

What starts with transgender patients is already expanding to:
– Neurodivergent individuals, flagged by tone or atypical language
– Disabled patients, flagged for noncompliance or high care costs
– Low-income Medicaid enrollees, tracked for "overutilization"
– Immigrants, flagged by cross-agency data fusion between Medicaid and ICE
– Political dissidents, whose digital speech is run through sentiment analysis tools

This infrastructure—risk matrices, escalation dashboards, AI-driven behavioral profiling—can be replicated by any insurer, health system, or corporate actor with access to patient data. It replaces clinical care with predictive policing. It replaces grievance resolution with biometric suspicion.

We are the first target. Not the last.

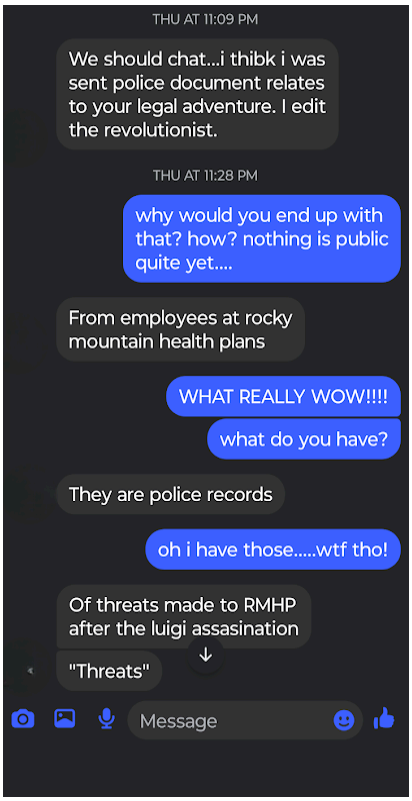
VIII. Internal Warnings Ignored: The Whistleblower Letter and the Culture of Suppression

At the point the letter reached the Plaintiff's friend—an independent journalist and editor of *The Revolutionist*—received an anonymous letter by mail. The envelope was unmarked, bore no return address, and has since been discarded. Only later, after reviewing the contents, did the friend contact the Plaintiff and provide her with photographs of what had been enclosed.

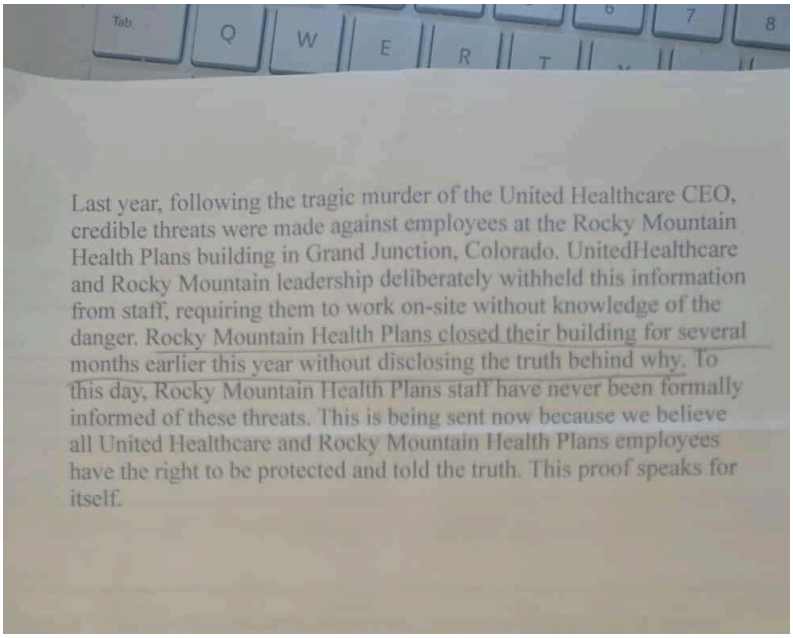
Those materials included:

- A typed, unsigned letter alleging internal suppression of credible threats made against Rocky Mountain Health Plans (RMHP) employees
- Several pages of redacted Grand Junction Police Department (GJPD) reports

According to the letter, some employees believed that the silence following the CEO's high-profile death was not coincidental. Internally, the resulting secrecy and building closure were allegedly referred to as "the aftermath"—a phrase suggesting institutional concealment rather than precaution.



(1)

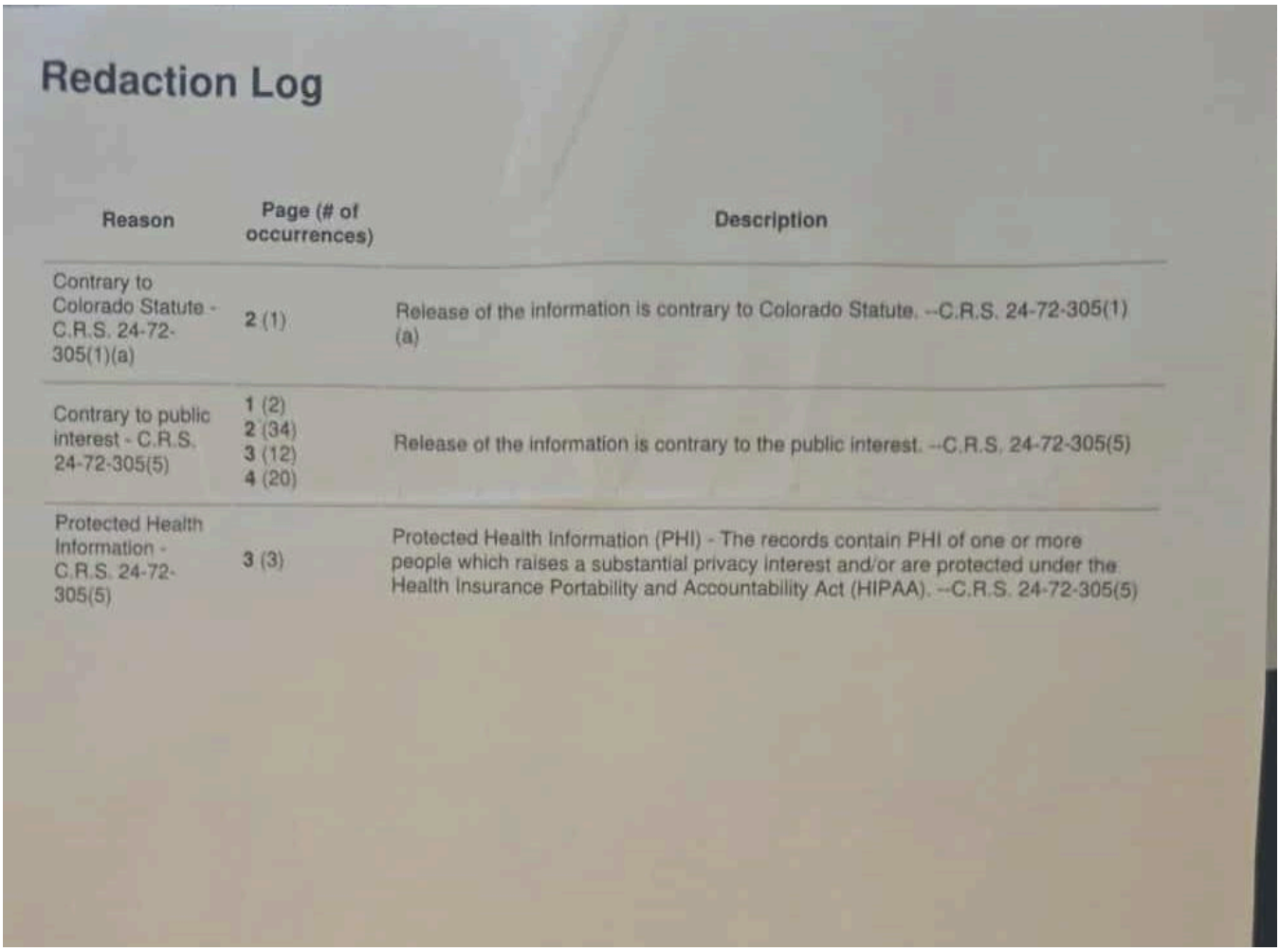


(2)

Figure 1 – Screenshot of original chat exchange confirming receipt of the whistleblower letter and police records by Plaintiff's friend (Image 1)

Figure 2 – Cropped image of whistleblower letter excerpt describing concealed threats to RMHP staff (Image 2)

The timing is significant. At the moment the letter reached the Plaintiff's friend, the Plaintiff had made no public statement, filed no legal complaint, and had published no metadata or investigative disclosures. This unsolicited mailing—arriving *before* any outward action—suggests deep internal awareness, fear, and systemic unease within UnitedHealthcare and RMHP.



Redaction Log

Reason	Page (# of occurrences)	Description
Contrary to Colorado Statute - C.R.S. 24-72-305(1)(a)	2 (1)	Release of the information is contrary to Colorado Statute. --C.R.S. 24-72-305(1)(a)
Contrary to public interest - C.R.S. 24-72-305(5)	1 (2) 2 (34) 3 (12) 4 (20)	Release of the information is contrary to the public interest. --C.R.S. 24-72-305(5)
Protected Health Information - C.R.S. 24-72-305(5)	3 (3)	Protected Health Information (PHI) - The records contain PHI of one or more people which raises a substantial privacy interest and/or are protected under the Health Insurance Portability and Accountability Act (HIPAA). --C.R.S. 24-72-305(5)

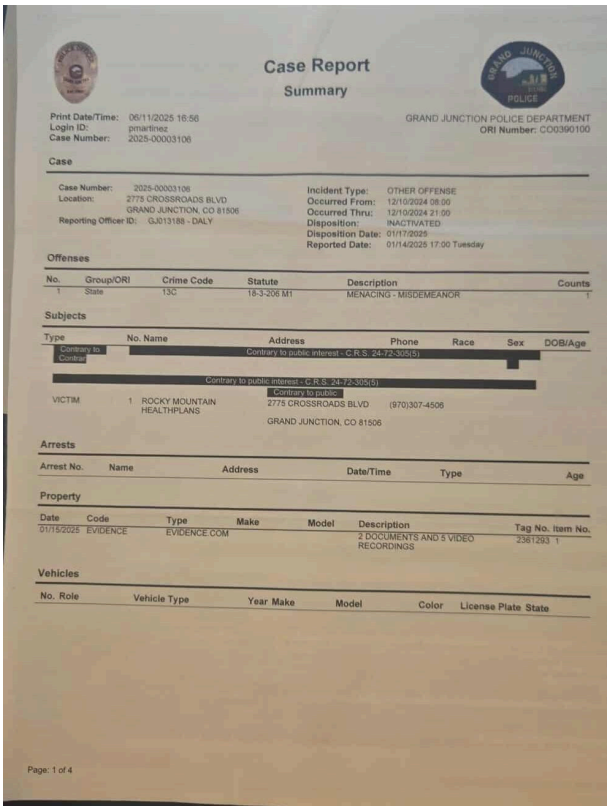
(3)

Figure 3 – Redaction Log from whistleblower packet showing use of HIPAA, C.R.S. 24-72-305(5), and public interest exemptions (Image 3)

The Plaintiff includes this disclosure not to validate every internal allegation, but to show that the same institutional behaviors she would later document—PHI misuse, law enforcement escalation, and algorithmic profiling—had already raised alarms inside the institutions themselves.

More tellingly, the redacted GJPD case files matched Plaintiff's later CORA-acquired records *exactly*, confirming:

- **The calls were lawful and concerned prescription access**
- **RMHP and UHC uploaded multiple call recordings to police**
- **HIPAA-protected health information was shared under 'public interest' justifications**
- **The police report numbers were identical across both sources**



Case Report
Summary

GRAND JUNCTION POLICE DEPARTMENT
ORI Number: CO0390100

Print Date/Time: 06/11/2025 16:56
Login ID: pmartinez
Case Number: 2025-00003106

Case

Case Number: 2025-00003106
Location: 2775 CROSSROADS BLVD GRAND JUNCTION, CO 81506
Reporting Officer ID: GJ013188 - DALY
Incident Type: OTHER OFFENSE
Occurred From: 12/10/2024 08:00
Occurred Thru: 12/10/2024 21:00
Disposition: INACTIVATED
Disposition Date: 01/17/2025
Reported Date: 01/14/2025 17:00 Tuesday

Offenses

No.	Group/ORI	Crime Code	Statute	Description	Counts
1	State	13C	18-3-206 M1	MENACING - MISDEMEANOR	1

Subjects

Type	No.	Name	Address	Phone	Race	Sex	DOB/Age
Contrary to Contrar		Contrary to public interest - C.R.S. 24-72-305(5)					
Contrary to public interest - C.R.S. 24-72-305(5)							
VICTIM	1	ROCKY MOUNTAIN HEALTHPLANS	Contrary to public 2775 CROSSROADS BLVD GRAND JUNCTION, CO 81506	(970)307-4506			

Arrests

Arrest No.	Name	Address	Date/Time	Type	Age

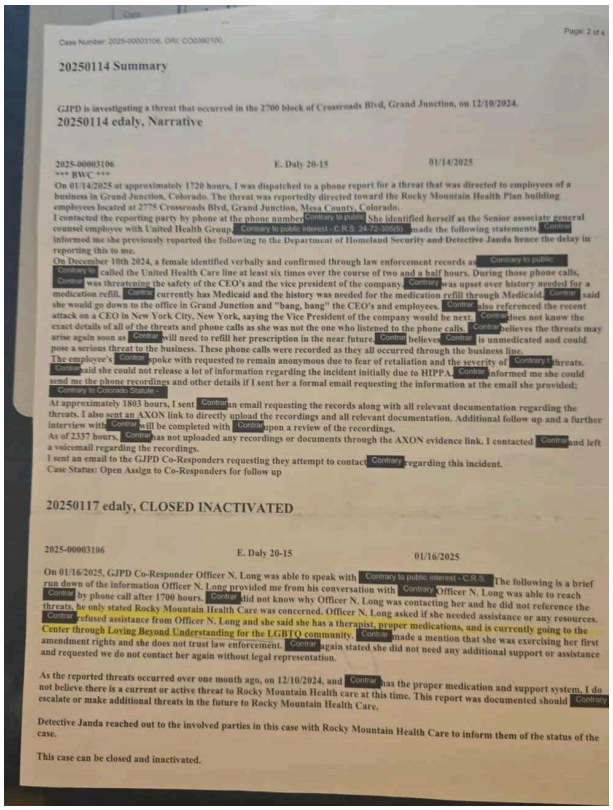
Property

Date	Code	Type	Make	Model	Description	Tag No.	Item No.
01/15/2025	EVIDENCE	EVIDENCE.COM			2 DOCUMENTS AND 5 VIDEO RECORDINGS	2361293	1

Vehicles

No.	Role	Vehicle Type	Year	Make	Model	Color	License Plate	State

Page: 1 of 4



Case Number: 2025-00003106, ORI: CO0390100

Page: 2 of 4

20250114 Summary

GJPD is investigating a threat that occurred in the 2700 block of Crossroads Blvd, Grand Junction, on 12/10/2024.

20250114 edaly, Narrative

2025-00003106 E. Daly 20-15 01/14/2025

*** BWC ***

On 01/14/2025 at approximately 1720 hours, I was dispatched to a phone report for a threat that was directed to employees of a business in Grand Junction, Colorado. The threat was reportedly directed toward the Rocky Mountain Health Plan building employees located at 2775 Crossroads Blvd, Grand Junction, Mesa County, Colorado.

I contacted the reporting party by phone at the phone number Contrary to public She identified herself as the Senior associate general counsel employee with United Health Group, Contrary to public interest - C.R.S. 24-72-305(5) made the following statements Contrar informed me she previously reported the following to the Department of Homeland Security and Detective Janda hence the delay in reporting this to me.

On December 18th 2024, a female identified verbally and confirmed through law enforcement records as Contrary to public Contrary to called the United Health Care line at least six times over the course of two and a half hours. During those phone calls, Contrar was threatening the safety of the CEO's and the vice president of the company. Contrary was upset over history needed for a medication refill. Contrar currently has Medicaid and the history was needed for the medication refill through Medicaid. Contrar said she would go down to the office in Grand Junction and "bang, bang" the CEO's and employees. Contrar also referenced the recent attack on a CEO in New York City, New York, saying the Vice President of the company would be next. Contrar does not know the exact details of all of the threats and phone calls as she was not the one who listened to the phone calls. Contrar believes the threats may arise again soon as Contrar will need to refill her prescription in the near future. Contrar believes Contrar is unmedicated and could pose a serious threat to the business. These phone calls were recorded as they all occurred through the business line.

The employee's Contrar spoke with requested to remain anonymous due to fear of retaliation and the severity of Contrary t threats. Contrar said she could not release a lot of information regarding the incident initially due to HIPPA. Contrar informed me she could send me the phone recordings and other details if I sent her a formal email requesting the information at the email she provided;

Contrary to Colorado Statute -

At approximately 1803 hours, I sent Contrar an email requesting the records along with all relevant documentation regarding the threats. I also sent an AXON link to directly upload the recordings and all relevant documentation. Additional follow up and a further interview with Contrar will be completed with Contrar upon a review of the recordings.

As of 2337 hours, Contrar has not uploaded any recordings or documents through the AXON evidence link. I contacted Contrar and left a voicemail regarding the recordings.

I sent an email to the GJPD Co-Responders requesting they attempt to contact Contrar regarding this incident.

Case Status: Open Assign to Co-Responders for follow up

20250117 edaly, CLOSED INACTIVATED

2025-00003106 E. Daly 20-15 01/16/2025

On 01/16/2025, GJPD Co-Responder Officer N. Long was able to speak with Contrary to public interest - C.R.S. The following is a brief run down of the information Officer N. Long provided me from his conversation with Contrar Contrary Officer N. Long was able to reach by phone call after 1700 hours. Contrar did not know why Officer N. Long was contacting her and he did not reference the threats, he only stated Rocky Mountain Health Care was concerned. Officer N. Long asked if she needed assistance or any resources. Contrar refused assistance from Officer N. Long and she said she has a therapist, proper medications, and is currently going to the Center through Loving Beyond Understanding for the LGBTQ community. Contrar made a mention that she was exercising her first amendment rights and she does not trust law enforcement. Contrar again stated she did not need any additional support or assistance and requested we do not contact her again without legal representation.

As the reported threats occurred over one month ago, on 12/10/2024, and Contrar has the proper medication and support system, I do not believe there is a current or active threat to Rocky Mountain Health care at this time. This report was documented should Contrary escalate or make additional threats in the future to Rocky Mountain Health Care.

Detective Janda reached out to the involved parties in this case with Rocky Mountain Health Care to inform them of the status of the case.

This case can be closed and inactivated.

(4) (5)

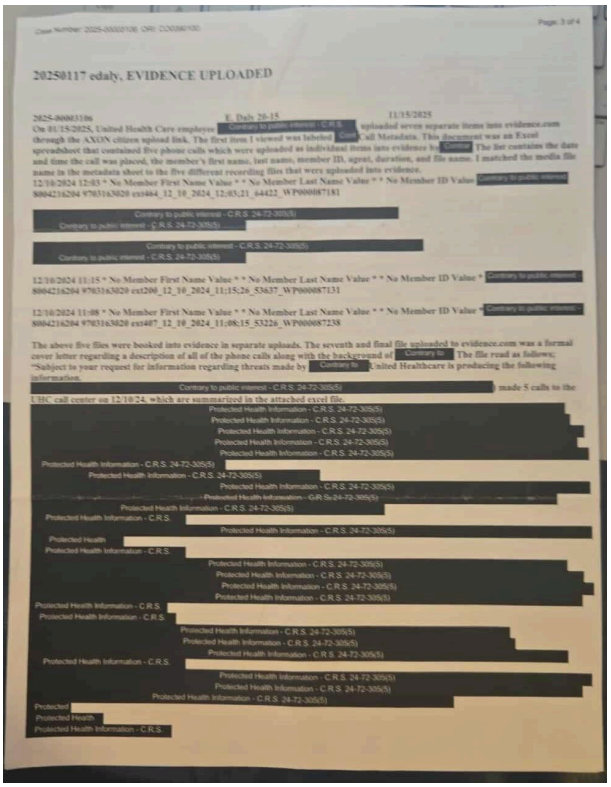
Figure 4 – GJPD Officer Narrative confirming Plaintiff was not threatening and that no criminal charges were filed (Image 4,5.6 and 7)

Figure 5 – GJPD case narrative, final summary, and inactivation order confirming the case was closed (Image 5)

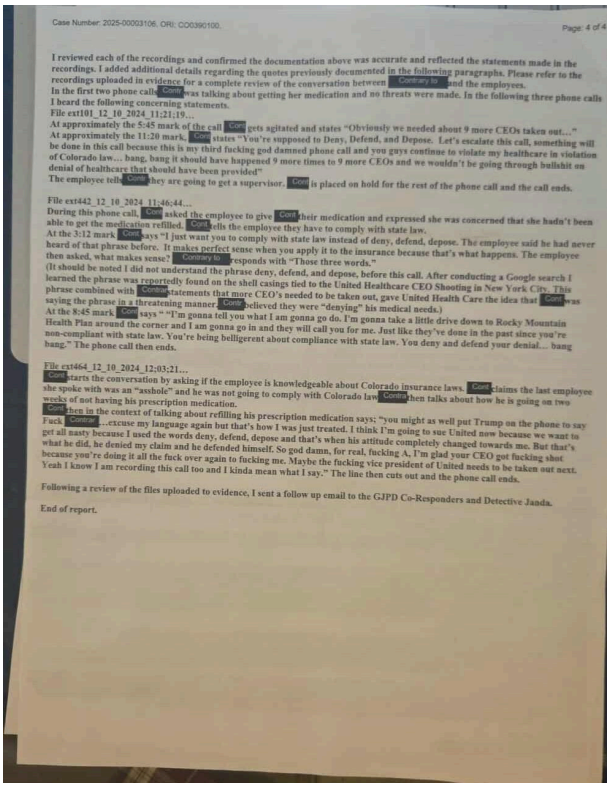
The fifth image, a redacted summary sheet from GJPD, confirms the case status:

- **Charge: Menacing – Misdemeanor (C.R.S. 18-3-206)**
- **Disposition: Inactivated**
- **Date Closed: 01/17/2025**
- **Final finding: No charges filed. Case closed.**

Figure 7 – GJPD Summary confirming language of the calls filed (Image 7)



(6)



(7)

The Plaintiff, Samara Dorn, was never arrested or charged. Police notes affirm she was *not* deemed a threat, was mentally stable, had adequate support, and refused additional intervention. **She was formally cleared.**

Thus, while the whistleblower letter reveals real institutional panic and an effort to conceal internal threats, it does **not** implicate the Plaintiff—nor should it ever be construed as doing so. If anything, it reinforces the central truth of her case:

> *She was not retaliated against because she was dangerous. She was retaliated against because she refused to disappear.*

Her metadata became the threat. Their silence became the liability. And the letter? It was not a warning. It was proof that someone inside had already lost faith in the system they were part of.

> "Someone already stopped believing in what we are."

VIII-A. Media Echo, Not Collusion: How an Escalation Became a Headline

Method note (defamation-safe framing). This section states opinion based on disclosed facts (records, exhibits, and the article itself). It critiques structure and timing and does not allege coordination. Readers are invited to evaluate the comparisons.

Litigation posture note. These observations are now directly relevant to *Dorn v. Grand Junction Daily Sentinel*, Mesa County District Court, Case No. 2025-CV-61, and contextual to *Dorn v. UnitedHealthcare et al.*, Case No. 2025-CV-73. No coordination is alleged; the focus is how structure and omission can generate a misleading gist "of and concerning" the Plaintiff in a small-market context.

What the public saw

On or about July 30, 2025, the *Grand Junction Daily Sentinel* ran a piece about a "threat-driven" RMHP office impact (archived Aug. 4, 2025, 03:27 UTC: [FN3]). The article did not name me, yet its presentation (headline/subhead, quote sequencing, and adjacency of unrelated case material) made two legally distinct matters read like one story. Police filed no charges on my December 2024 call; the referral was inactivated within days—facts that appeared, but not as the frame.

Identification without naming. In smaller markets, unique combos of dates, descriptors, role, and phrasing can render a person reasonably identifiable (the mosaic/jigsaw effect). Under **defamation-by-implication** doctrine, harm turns on the gist and whether a publication is "of and concerning" the plaintiff to those who know the context. Structure can imply what no sentence states.

Five narrative mechanics that convert escalation into "threat"

- Composite persona. Back-to-back paragraphs about different people feel like one subject unless loudly disambiguated.
- Redaction asymmetry. Official-looking snippets shed the context that cleared the patient.
- Temporal elasticity. Months-apart events read "immediate" when stacked.
- Quote laundering. Therapeutic/rhetorical lines (e.g., "deny, defend, depose") sound like intent stripped of clinical/advocacy context.
- Headline gravity. A sensational subhead out-weights later caveats ("no ongoing threat").

None of this proves coordination; together it shows how upstream privacy breaches re-emerge as downstream stigma—even unnamed.

Side-by-side chronology (reader inference encouraged)

- Dec 2024: last call about denied medication; expressive phrases; no threats.
- Jan 14–15, 2025: insurer referral & voluntary PHI transmission; five audio files; no subpoena/warrant.
- Jan 17, 2025: law enforcement inactivates; no charges.
- July 30, 2025: article publishes (unnamed subject); two matters juxtaposed; clearing facts de-emphasized.

Inference: the timing/structure let an inactivated referral live on as a community-safety narrative.

Plausible (non-accusatory) sourcing pathways

Models, not claims: (1) redacted public records; timelines fused inadvertently. (2)

law-enforcement paraphrase; caveats buried. (3) routine PR/background; framing nudged without PHI. (4) independent witness memory; gaps filled by recall. Discovery—not this article—tests which fits.

Process questions (neutral, not accusatory)

- Did notes mark two subjects/timelines and require explicit disambiguation?
- What source hierarchy (docs vs. paraphrase) drove the subhead?
- Were clearing facts (no charges/inactivated) eligible for headline/snippet placement?
- Was re-identification risk assessed given the specificity of dates, descriptors, and quotes?

Counterfactual fairness test

If the patient were cisgender, neurotypical, and not post-op denied, would quotes and sequencing be the same? If "no charges/inactivated" led, would the public gist change? Editorial—not legal—questions flag implicit-bias risk.

Re-identification risk: anonymity is porous

Distinctive combos—surgery type, call timing, phrasing, insurer, locale—can ID someone even unnamed. De-identification isn't just removing a name; it's reducing linkable descriptors. Practical takeaway: foreground clearing facts, consolidate dates into ranges, avoid distinctive quotes never criminalized.

What fair framing could have looked like (illustrative)

- Lede: "Police reviewed two unrelated matters; in one, authorities found no ongoing threat and closed it within days."
- Structure: Two clearly labeled sub-sections—"Matter A (closed; no charges)" and "Matter B (separate subject)."
- Context box: "Therapeutic/rhetorical speech ≠ intent; police did not pursue charges."

Remedies short of blame

- Clarification note: affirm two matters; one closed with no charges.
- Update banner: side-by-side timeline graphic.
- Search snippet control: surface "no ongoing threat/closed" in the first ~160 characters.

Why this matters beyond one story

When a voluntary insurer disclosure seeds police files and reappears in print as a threat narrative, administrative misclassification hardens into community stigma, chilling appeals and care-seeking—especially for transgender and neurodivergent patients.

Editor's Note. Commentary and fair critique grounded in disclosed materials; no allegation of collusion; goal is accuracy with minimized harm.

VIII-A-1. Structural Forensics (Exhibit D, summarized — opinion based on disclosed facts)

Scope & standard. Good-faith media critique from disclosed materials (police records, the article, exhibits). Focus: presentation mechanics, not motive. No coordination alleged.

Litigation posture note. These observations are directly relevant to *Dorn v. Grand Junction Daily Sentinel*, Case No. 2025-CV-61 (defamation by implication/"gist"), and also contextual to *Dorn v. UnitedHealthcare et al.*, Case No. 2025-CV-73, which challenges the insurer's upstream disclosures that seeded the reputational echo.

A) Fusion & proximity misattribution

• Subject blending. Unmarked switches (generic "she/they/the individual") can collapse two cases into one composite persona.

• Temporal compression. Weeks-apart events read as "now" when stacked without date flags.

• Quote adjacency. Unattributed lines between Subject A and B invite the assumption the same person said it; therapeutic/activist phrases read like intent when crisis context is missing.

B) Headline gravity vs. buried exculpation

A charged subhead anchors memory; deep-body caveats ("no charges," "inactivated") can't fully correct the initial gist.

C) Omission patterns that magnify harm (without saying anyone lied)

• Missing separators/labels between cases over-associates conduct from B to A.

• Absent clinical context (post-op denial, timing gap) removes why speech sounded distressed.

• No conflict-context (pending litigation/notice) leaves readers blind to source incentives.

D) "Mosaic ID" risk: unnamed ≠ unidentifiable

Distinctive combos (surgery, date ranges, insurer, signature phrasing) can ID a person locally; editorial choices on how many specifics matter.

E) Fairness-first counter-layout (illustrative)

• Lede: two matters; one closed with no charges.

• Structure: "Matter A (closed)" / "Matter B (separate subject)."

• Inline flags: date stamps on each subject switch; repeated "different subjects" reminders.

F) Process questions that improve accuracy

• Did the newsroom run a re-ID check for the unnamed subject?

• Were clearing facts eligible for headline/snippet, not just late-paragraph placement?

G) Remedies without conceding fault

• Clarification note + timeline graphic; adjust preview to surface "closed/no charges."

• Style-guide addendum for PHI-adjacent content: "clearing facts first," subject-switch labels, and a re-ID risk pass.

H) Why this belongs in a HIPAA/civil-rights analysis

When voluntary PHI-adjacent disclosures seed law-enforcement files and reappear as threat

narratives via structure/omission, a privacy breach becomes a durable reputational penalty that chills care-seeking, appeals, and advocacy speech.

Editor's Note. Forensic subsection offered as commentary on structure/timing/reader impact; no collusion asserted; purpose is improving accuracy while minimizing avoidable harm.

VIII-A-2. Colorado Defamation Posture — Anti-SLAPP, Fair-Report, and "Gist" (No False-Light)

Sources for this subsection: [FN1] (CV-61 filings), [FN3] (archived article), [FN4] (Colorado does not recognize false light), [FN5] (Coomer / Anti-SLAPP).

Litigation posture. These observations frame the defamation claims now pending in *Dorn v. Grand Junction Daily Sentinel* (Mesa County District Court, Case No. 2025-CV-61). Colorado does not recognize false-light; the theory proceeds under **defamation (including implication by structure and materially false "gist")**. Evidence references are contained in the case record.

A) What's actionable here (element-by-element checklist).

1. **Material falsity / "gist."** The publication conveyed a materially false impression by: (i) fabricating a sensational subhead not found in any record, (ii) misattributing quotes from a different matter to the Plaintiff, and (iii) fusing separate incidents into a single "female perpetrator" narrative while burying exculpatory facts (no charges; referral inactivated within days). These are falsifiable assertions, not protected opinion.
2. **"Of and concerning."** Identification is satisfied even without naming when readers in a small market can recognize the Plaintiff via mosaic identifiers (distinctive phrasing, gendered references, dates, insurer, locale).
3. **Publication.** The article published on or about July 30, 2025 and remains archived [FN3].
4. **Fault.** At minimum, negligence in assembling a composite persona and misplacing quotes; discovery will test knowledge of contradictions and disregard of clearing facts.
5. **Damages.** Predictable re-identification and stigmatization in a small community; chilling effects on care-seeking and speech—harms consistent with defamation by implication.

B) Fair-report privilege has limits.

Colorado's fair-report privilege protects fair and accurate accounts of official proceedings. It does not shield editorial inventions, misattributions, or distortions that alter the sting of the story. Invented headlines/subheads, misassigned quotes, and omitting clearing findings (no threat; no charges; case inactivated) defeat the privilege because the net impression ceases to be fair or accurate.

C) Anti-SLAPP (C.R.S. § 13-20-1101) — why these claims clear Prong Two.

Colorado's Anti-SLAPP uses a two-step: (1) speech on a matter of public concern; and (2)

whether the plaintiff shows a reasonable likelihood of prevailing. At step two, courts accept the plaintiff's evidence as true, do not weigh credibility, and ask whether the plaintiff can probably meet their trial burden (including clear-and-convincing actual malice where applicable). Appellate review is de novo. See **Coomer v. Salem Media of Colorado, Inc.**, 2025COA2, No. 23CA1235 (Colo. App. Jan. 16, 2025) [FN5].

• Prong One is typically assumed for newsroom reporting.

• Prong Two is satisfied here by the record buckets already documented: fabrication, misattribution, composite fusion, buried exculpation, plus the mosaic ID showing "of and concerning." Those categories map directly to falsity, identification, fault, and damages.

D) What this subsection is not.

It is not an allegation of collusion. It is a structure-and-records critique explaining why defamation (gist/implication) survives both fair-report and Anti-SLAPP at this stage.

IX. Algorithmic Surveillance and Escalation: When AI Classifies Identity as Instability

In the Plaintiff's case, UnitedHealthcare did not respond to a transgender member's distress with care. It responded with **classification**.

According to the **Final Filed Complaint** and the attached records (including GJPD narrative logs and exhibit materials), UnitedHealthcare and Rocky Mountain Health Plans collected, analyzed, and shared the Plaintiff's audio recordings, psychiatric medication list, surgical history, and protected political speech with police—**without** a warrant, court order, subpoena, or exigent medical justification. These disclosures occurred approximately **thirty-five (35) days** after the final phone call, raising serious constitutional and statutory concerns. If proven, that timing cannot satisfy HIPAA's "**serious and imminent threat**" standard under 45 C.F.R. § 164.512(j).

Rather than treat the Plaintiff's voice as one seeking redress for an unlawful medication denial, UnitedHealthcare appears to have re-framed her speech as **reputational risk**. The Plaintiff alleges that her calls—expressing despair, anger, and frustration after being denied access to a pre-approved hormone therapy—were analyzed and escalated not by human discretion but through automated systems, likely including tools such as **CallMiner Eureka**. Across the healthcare industry, such tools are marketed as "AI-powered analytics" to reduce churn, improve compliance, and manage escalation events. For patients like the Plaintiff—neurodivergent, trans, and post-operative—these systems often cannot parse **distress vs. danger**, **protest vs. threat**, or **trauma vs. noncompliance**.

A Voice Misclassified

In her final December 2024 call to UnitedHealthcare, the Plaintiff referenced administrative injustice, expressed rage over being denied critical medication, and

invoked rhetorical slogans such as *"Deny. Defend. Depose."* Nowhere did she threaten violence. Nowhere did she indicate intent to harm herself or others.

As reflected in the **Final Filed Complaint, Mesa County District Court, Case No. 2025-CV-73**, and the **GJPD narrative log (Jan. 14, 2025)**, a UnitedHealthcare representative explicitly acknowledged HIPAA constraints to police, stating she *"could not release a lot of information… due to HIPAA."* Despite that acknowledgment—and with no legal process in place—Defendants voluntarily disclosed the Plaintiff's voice recordings, psychiatric references, transgender identity, and surgical history the next day.

If proven, this sequence would contravene **45 C.F.R. § 164.502(a)**, which limits uses and disclosures of protected health information (PHI) to those explicitly permitted or required by the Privacy Rule. The roughly thirty-five (35) day delay between the last call and the police referral also undercuts any reliance on **§ 164.512(j)**'s exception for a *"serious and imminent threat."*

Further, the Complaint alleges that Defendants failed to comply with the procedural safeguards for disclosures to law enforcement under **§ 164.512(f).** The police request was informal—via email—not a valid subpoena or formal legal demand. On the face of the records, the transmission was voluntary, not compelled.

Finally, the materials indicate that—even after acknowledging HIPAA limits and characterizing the Plaintiff's expressive speech as discomforting, not criminal—staff proceeded to transmit records. The result was a breach of trust wherein metadata escalation, not emergency care, appears to have triggered disclosure.

This is corroborated by **UnitedHealthcare's January 15, 2025 cover letter to the Grand Junction Police Department (Exhibit L),** which outlines the transmission of five recorded call summaries, including patient name, surgery type, medication, date of birth, and internal commentary about the Plaintiff's tone and rhetorical language. Nowhere does the letter cite a subpoena or court order. It describes the statements at issue as speculative or rhetorical, made during emotionally distressed calls about medication access—not specific threats or crimes under Colorado law.

Taken together, the Complaint, the **GJPD logs**, and **Exhibit L** support the inference that the Plaintiff's speech was routed through institutional escalation protocols that flagged her not as a patient in distress but as a potential institutional liability. In this analysis, her emotional tone, word choice, and identity likely triggered algorithmic scores used internally to route cases into reputational-risk workflows.

Citation note. References to the Final Filed Complaint are to **Case No. 2025-CV-73.** Paragraph numbers are intentionally omitted; all supporting records are available in the court docket and in the Plaintiff's public case archive.

Exhibit L – UHC Cover Letter to Grand Junction Police

UNITEDHEALTH GROUP

Contrary to public interest - C.R.S. 24-72-305(5)

January 15, 2025

Det. Tim Janda
Advanced Real Time Information Center Investigations Division
Grand Junction Police Department
555 Ute Ave.
Grand Junction, CO 81501

Subject to your request for information regarding threats made by Samara Dorn, UnitedHealthcare is producing the following information.

Samara Dorn (DoB [redacted], Address: [redacted] Fruita, CO 81521; Phone number (970) [redacted]) made 5 calls to the UHC call center on 12/10/24, which are summarized in the attached excel file.

Dorn had gender affirmation surgery and was calling about post-op estrogen medication. Her doctor had submitted it for a prior authorization, as required by Colorado state Medicaid regulations (despite Dorn's protestations to the contrary – Dorn incorrectly asserts at several different points during the calls that UHC is required to cover the medication without prior authorization). Because the dosage requested in the PA was at a high level, UHC initially denied the prior authorization while it requested more information from Dorn's doctor. That prompted the following calls from Dorn to various call center personnel (in chronological order per the time stamps on when they happened on 12/10/2024):

File ext407_12_10_2024_11;08;15… (Dorn's initial call into UHC/ORx)

- Per Dorn, at roughly the 3:30 mark, the medication is "estradiol valerate" and the Colorado "law" that requires coverage is "Colorado department of healthcare policy and financing gender affirming care manual." Dorn mistakenly believes that the medication is "covered under tier 2 per the medication coverage guide" without prior authorization.

File ext200_12_10_2024_11;15;26…

- This is actually a call between a UHC advocate and an OptumRx advocate where the UHC advocate is trying to work with ORx to help Dorn (who is on hold).

File ext101_12_10_2024_11;21;19…

- At approximately the 5:45 mark of the call Dorn gets agitated and states "Obviously we needed about 9 more CEOs taken out…"
- At approximately the 11:20 mark, Dorn states "Deny, Defend, and Depose … let's escalate this call, something will be done in this call because this is my third fucking god damned phone call … bang, bang it should have happened 9 more times to 9 more CEOs"

Exhibit L – UHC Cover Letter to Grand Junction Police Department

File ext442_12_10_2024_11;46;44…

- At the 1:20 mark, the advocate asks Dorn to please not curse on the phone or he will be forced to disconnect the call.
- At the 3:12 mark Dorn says "deny, defend, depose… it makes perfect sense when you apply it to … you guys [UHC]"
- At the 8:45 mark Dorn says "I'm going to go down to RMHP … you're being belligerent in your deny and defend… bang bang."

File ext464_12_10_2024_12;03;21…

- Starting at about the 2:50 mark Dorn starts a rant that includes: "put Trump on the phone to say Fuck Samara … I think I'm going to sue United now because you're going to get all nasty now because I used deny, defend, depose … I'm glad your CEO got fucking shot … maybe the fucking vice president of United needs to be taken out next … I kinda mean what I say."

Sincerely,

Contrary to public interest - C.R.S. 24-72-305(5)

Surveillance Disguised as Care

The Plaintiff's **Final Filed Complaint, Mesa County District Court, Case No. 2025-CV-73**, identifies that no medical professional reviewed her case before escalation. No crisis referral was made. No welfare support was offered. Instead, her metadata was bundled and handed to law enforcement. What reached police, according to the Complaint and attached records, was not a clinical report but a selectively redacted, internally written justification framed around *"safety,"* devoid of any direct threat.

Discovery **to be served** in this matter will seek to confirm the role of automation in that process. Among the anticipated requests:

- **Requests for Admission (draft Nos. 112, 114–115)** will ask Defendants to admit whether at least one automated system, algorithm, or AI-based tool contributed to the risk assessment, escalation, or internal classification of the Plaintiff's calls, and whether gender identity, race, disability, or neurodivergence were modeled as escalation

variables.

- **Interrogatory (draft No. 28)** will ask Defendants to identify and describe all escalation matrices or AI threshold tools used to decide when a patient is routed to Legal or Security.
- **Requests for Production (draft Nos. 67–71)** will seek training materials, risk protocols, and behavioral scoring guides used to justify law-enforcement disclosures.

These draft requests track the central allegation: that the Plaintiff's transgender identity and neurodivergent communication style were misread by surveillance systems not trained to recognize legitimate protest, trauma-affected speech, or disability accommodations.

Citation note. References to the Final Filed Complaint are to **Case No. 2025-CV-73.** Paragraph numbers are intentionally omitted; discovery identifiers refer to draft requests prepared for service in this matter.

Administrative Risk by Algorithm

This surveillance infrastructure is not unique to the Plaintiff's case. It reflects a broader industry trend: administrative actors replacing clinical discretion with predictive analytics, risk matrices, and AI-based compliance flagging.

As alleged in the **Final Filed Complaint, Mesa County District Court, Case No. 2025-CV-73**, UnitedHealthcare deployed automated scoring systems—likely including tools such as *CallMiner Eureka*—to evaluate the Plaintiff's speech for volatility, sentiment, and reputational risk. These systems are widely marketed as *"AI-powered analytics"* to reduce churn, improve compliance, and manage escalation events. But in practice they are error-prone around marginalized patients: protest reads as threat, neurodivergence as noncompliance, identity as instability.

Consistent with the Complaint and exhibits, the escalation timeline and content of the disclosures indicate that the Plaintiff's calls were processed not through human clinical judgment, but through algorithmic flagging protocols designed to protect the institution—not the patient. The result was **administrative risk by algorithm**: a workflow where tone, trauma, and identity became inputs to a reputational-risk engine, routing a patient in distress away from care and into a police narrative.

Citation note. References to the Final Filed Complaint are to **Case No. 2025-CV-73.** Paragraph numbers are intentionally omitted; supporting records are available in the court docket and in the Plaintiff's public case archive.

When a patient exhibits frustration, their call is no longer reviewed by a care advocate. It is scored by software.

This automation breaks down in three dangerous ways:

- **Disability Erasure** – Autistic, neurodivergent, or mentally ill patients are flagged as volatile, noncompliant, or reputational threats due to vocal tone, pacing, or content that deviates from neurotypical expectations.
- **Identity Profiling** – Transgender patients, particularly those invoking political or trauma-informed language, are seen as disruptive rather than harmed. Their gender identity becomes a perceived risk signal rather than a clinical context.
- **Due Process Collapse** – Once flagged, there is no known appeals process. No patient is informed their metadata is being routed for risk escalation. No legal notice is given. The result is a quiet transfer of PHI to law enforcement, outside the bounds of warrant, consent, or public scrutiny.

Digital Profiling as a Mechanism of Retaliation

This section of the record supports the Plaintiff's broader thesis: that she was not treated as a patient. She was profiled as a threat. Not for what she did, but for who she was—and how she spoke.

Her metadata did not indicate criminality. It indicated rage, protest, and political identity. And in the post-2024 environment of anti-trans surveillance, that was enough.

The Plaintiff is not alleging a technical HIPAA mishap. She is alleging that a multinational healthcare corporation used AI systems to suppress a patient's protected identity and speech under the pretext of internal security—and that this suppression was routed, deliberately, into a police narrative.

When systems cannot distinguish between trauma and danger, when protest is categorized as escalation, and when speech is algorithmically converted into risk metadata, care ceases to be care. It becomes surveillance. And in the Plaintiff's case, it became retaliation.

X. CONCLUSION: This Is the Fight They Wanted to Avoid

"My silence will not protect me." — Audre Lorde

UnitedHealthcare made a calculated bet: that I, a trans woman in distress, would be too destabilized to respond. That I would shrink from confrontation. That I would absorb the harm, accept the stigma, and vanish under the weight of institutional force. That I would not fight back—because the machine was designed to outlast me.

They were wrong.

This case is not about a singular act of harm—it is about a system that punishes identity, pathologizes dissent, and exploits metadata as a proxy for control. It is about what happens

when care becomes surveillance, and when bureaucracies weaponize silence as a shield against accountability.

I am not a one-off anomaly. I am a signal flare in a system built on selective erasure. I speak not only for myself, but for the 3.3 million trans Americans whose lives are routinely redacted, reclassified, and routed into administrative nonexistence. Whose very existence is treated as a compliance issue rather than a civil right. Whose gender is considered negotiable if it interferes with cost control, actuarial modeling, or executive comfort.

I reject that premise.

I will not accept that my identity is a threat vector. I will not be told that my voice is too political to be protected. I will not be managed out of existence to preserve a ledger, a brand, or a bureaucracy.

This is not merely a policy violation. This is a denial of personhood.

Because if they can flag my distress as a justification for escalation—if they can redefine protected speech as volatility—if they can route a trans woman into a police encounter based on suppressed metadata—

Then none of us are safe.

This isn't just litigation. This is what accountability looks like when the system hopes you won't survive long enough to demand it.

This is not vengeance. This is not instability. This is not a fluke.

"This is resistance. This is survival. This is the record."

And when this document is found in their inbox, in their boardroom, in their legal file—let it also be found in their conscience.

This is my life.
And it will not be erased quietly.

— Samara Dorn, Plaintiff
www.AdministrativeErasure.org
– A Bureaucratic Hit Job Exposed

Author Note: Samara Dorn is a transgender pro se litigant in an ongoing HIPAA, privacy, and civil rights case. This commentary draws from her firsthand experience, legal filings, metadata logs, and internal correspondence from UnitedHealthcare and Rocky Mountain Health Plans. All content is documented, peer-verifiable, and protected under doctrines of academic freedom and public interest speech.

🔧 Footnotes

FN1. Master filings archive for *Dorn v. Grand Junction Daily Sentinel*, Mesa County District Court, Case No. 2025-CV-61: https://drive.google.com/drive/folders/1D3-LxxYbHRDyXI0KVzNUhF5DLnreUzBc

FN2. Master filings archive for *Dorn v. UnitedHealthcare et al.*, Mesa County District Court, Case No. 2025-CV-73: https://drive.google.com/drive/folders/1otDtRhl9rVgMLzlG0EcbxN1zC0O3zC_j

FN3. Archived version of *Grand Junction Daily Sentinel* article: https://web.archive.org/web/20250804032730/https://www.gjsentinel.com/news/western_colorado/threats-to-rocky-mountain-health-plans-caused-four-month-office-closure/article_12e06d9d-4594-4ada-9985-eb1e0dd99515.html

FN4. Authority note: Colorado does **not** recognize false-light; claims proceed under **defamation/defamation by implication (gist)**.

FN5. Coomer v. Salem Media of Colorado, Inc., 2025COA2, No. 23CA1235 (Colo. App. Jan. 16, 2025), **Order Affirmed in Part and Reversed in Part** (plaintiff met Anti-SLAPP Prong Two on defamation & IIED; conspiracy dismissed). PDF: https://www.coloradojudicial.gov/system/files/opinions-2025-01/23CA1235-PD_0.pdf