FREEDOM TO OPERATE ANALYSIS

ANVIL

Continuous Prescriber Biometric Presence Attestation System
for DEA Telehealth Compliance

Prepared for: XORD Systems LLC
Date: May 17, 2026
Classification: CONFIDENTIAL — Attorney-Client Privilege Applies

1. EXECUTIVE SUMMARY

This Freedom to Operate (FTO) analysis evaluates the patent landscape surrounding ANVIL's core technology: continuous biometric prescriber presence attestation during telehealth consultations for controlled substance prescribing. The analysis covers granted US patents and published applications from 2015–present across four technical vectors: (1) continuous/session-based biometric verification, (2) telehealth prescriber identity verification, (3) cryptographic healthcare audit trails, and (4) anti-spoofing/PAD in video.

Risk Level	Category	Assessment
[GREEN]	Combined System	No blocking patent identified covering the integrated ANVIL architecture
[YELLOW]	Continuous Session Auth (Sub-component)	Generic continuous auth patents exist but lack telehealth/DEA specificity
[YELLOW]	PAD/Liveness Detection (Sub-component)	Vendor patents (iProov Flashmark, BioID, FaceTec) on specific PAD methods
[GREEN]	Cryptographic Audit (DEA-format)	DEA audit formatting is regulatory compliance, not patented method
[GREEN]	Prescriber Presence Attestation	No patent found claiming biometric presence attestation linked to Rx auth

Bottom Line: ANVIL's integrated architecture—continuous 3D facial geometry polling during telehealth sessions, real-time embedding matching against enrolled biometric templates, cryptographic signing of session logs with DEA-compliant formatting, and auto-termination upon presence loss—occupies a novel intersection that no identified patent fully covers. The system's novelty lies in the combination of these elements in the specific context of DEA-regulated prescriber verification during live telehealth consultations. Individual sub-components (continuous face auth, liveness detection, cryptographic logging) have prior art, but none integrate them for prescriber presence attestation tied to controlled substance authorization.

2. CLAIM CHART MATRIX — RELEVANT PATENTS IDENTIFIED

2.1 US 12,192,199 — Continuous Session Authentication & Monitoring

Assignee: Paravision (FKA Kairos AR, Inc.)

Filed: March 6, 2019 | Granted: January 7, 2025

Expiration: ~March 2039

Claim Element	ANVIL Mapping	Risk Assessment
Authenticating a session for a user based on authentication image data structure and video frames	ANVIL authenticates prescriber via enrolled biometric template and live video frames	**[YELLOW]** Conceptual overlap on video-based session authentication
Extracting sample data from monitor region for second video frames; generating motion data	ANVIL performs continuous 3D facial geometry polling from video stream	**[YELLOW]** Monitoring-state concept overlaps, but ANVIL uses 3D geometry not 2D motion regions
Detecting re-authentication trigger event based on motion data	ANVIL auto-terminates on presence loss rather than re-authenticating on motion trigger	**[GREEN]** Different trigger mechanism (absence vs. motion anomaly)
No claims to: telehealth, prescriber verification, DEA compliance, controlled substances, or audit logging	ANVIL is purpose-built for DEA telehealth prescriber compliance with cryptographic audit trail	**[GREEN]** Entirely different field of use and regulatory context

Overall Assessment: YELLOW. Generic continuous session auth with facial video. No telehealth or healthcare claims. Doctrine of equivalents risk is low because ANVIL's architecture diverges on trigger mechanism (absence-based termination vs. motion-based re-auth) and uses 3D geometry rather than 2D sample regions. No literal infringement.

2.2 US 11,159,520 — Passive Continuous Session Authentication

Assignee: Paravision (same family as US 12,192,199)

Filed: March 6, 2019 | Granted: October 26, 2021

Expiration: ~March 2039

Same patent family as 12,192,199. Covers passive authentication combining biometric attributes from video with behavioral attributes from sensor data. ANVIL does not use behavioral biometrics (accelerometers, touch patterns). Risk is lower than the parent patent.

Overall Assessment: YELLOW-LOW. Behavioral biometric claims do not map to ANVIL. Only facial video component overlaps generically.

2.3 US 11,636,187 — Continuous User Authentication (Acronis)

Assignee: Acronis International GmbH

Filed: December 17, 2019 | Granted: April 25, 2023

Expiration: ~December 2039

Claims continuous authentication using heterogeneous data streams during communication sessions. Checks that the same person remains present throughout. General-purpose (not healthcare-specific).

Overall Assessment: YELLOW-LOW. Broad claims but no specificity to telehealth, prescriber verification, DEA compliance, or controlled substance authorization. Design-around: ANVIL's specific polling mechanism (isochronous 3D geometry at defined intervals) and DEA-specific audit binding distinguish it.

2.4 US 6,111,517 — Continuous Video Monitoring Using Face Recognition (Visionics/Identix)

Assignee: Visionics Corporation (now Idemia)

Filed: December 29, 1997 | Granted: August 29, 2000

Expiration: EXPIRED (~2017)

Pioneer patent on continuous face recognition for computer access control. Tracks authorized individual via video camera, revokes access when individual leaves field of view. This is prior art that actually validates ANVIL's core concept of presence-based auto-termination.

Overall Assessment: GREEN. Expired. Serves as prior art establishing the general concept of continuous face-based presence verification with access revocation, which helps ANVIL's freedom to operate.

2.5 US 7,847,815 — Facial Recognition in Video Conferences (Cisco)

Assignee: Cisco Technology, Inc.

Filed: October 11, 2006 | Granted: December 7, 2010

Expiration: ~October 2026 (nearing end)

Covers facial recognition of video conference participants for identification purposes (matching faces to stored images in a directory database). One-time identification at session join, not continuous monitoring. No authentication/access control claims, no healthcare context.

Overall Assessment: GREEN. One-time identification only, not continuous auth. Nearing expiration. No overlap with ANVIL's continuous attestation architecture.

2.6 US 9,106,789 — Videoconference and Video Visitation Security (Securus/Global Tel*Link)

Assignee: Global Tel*Link Corporation

Filed: 2012 | Granted: August 18, 2015

Expiration: ~2032

Covers continuous face detection and facial recognition during video visitation sessions in correctional facilities. Includes defacing areas outside detected faces, validating authorized visitors, and taking corrective action when unauthorized faces appear. Closest architectural analog to ANVIL in terms of continuous video-session face monitoring with enforcement action.

Claim Element	ANVIL Mapping	Risk Assessment
Detecting face in video stream during video visitation session	ANVIL detects prescriber face in video stream during telehealth session	**[YELLOW]** Conceptual parallel

Performing facial recognition; retrieving visitation record with facial characteristics	ANVIL matches against enrolled biometric templates	**[YELLOW]** Similar matching concept
Taking corrective action when unauthorized faces detected; continuous/periodic detection	ANVIL auto-terminates on presence loss	**[GREEN]** ANVIL terminates on absence, not unauthorized presence; different trigger
Defacing video areas outside detected face (privacy masking)	ANVIL does not perform video defacing/masking	**[GREEN]** Not applicable
Limited to correctional facility visitation context	ANVIL operates in DEA telehealth prescriber compliance context	**[GREEN]** Entirely different field of use

Overall Assessment: YELLOW-LOW. Closest structural analog but claims are specific to correctional video visitation with privacy masking. No healthcare, prescriber, or DEA claims. ANVIL's 3D geometry polling, embedding matching, cryptographic audit signing, and DEA-format logging are all unclaimed. No literal infringement. Doctrine of equivalents risk is minimal given the entirely different field of use.

2.7 US 10,366,217 — Continuous User Authentication (SecuredTouch/Ping Identity)

Assignee: SecuredTouch (acquired by Ping Identity)

Granted: July 30, 2019

Behavioral biometrics for continuous authentication on touchscreen devices. Analyzes user interaction patterns to differentiate humans from bots. No facial recognition component. No video analysis. No healthcare context.

Overall Assessment: GREEN. No technical overlap with ANVIL. Behavioral touch patterns vs. facial geometry.

2.8 US 11,184,766 — Continuous Authentication, Identity Assurance & Access Control (Callsign)

Assignee: Callsign, Inc.

Granted: November 23, 2021

Ambient authentication using behavioral analysis and environmental signals (WiFi, Bluetooth, GPS, pressure, humidity). Continuously verifies identity claims and intentional access. No facial biometric claims, no video analysis, no healthcare context.

Overall Assessment: GREEN. Ambient/environmental signal approach has no technical overlap with ANVIL's video-based facial geometry system.

2.9 US 12,112,849 — Safety Features for Medical Devices Requiring Supervision (Baxter/Fresenius)

Assignee: Fresenius Medical Care Holdings, Inc.

Granted: October 8, 2024

Covers continuous presence verification of an authorized helper during dialysis treatment sessions. Uses biometric authentication, video camera monitoring, and auto-termination (failsafe mode) when helper presence is not confirmed at predefined intervals. Reports to remote supervisor via internet.

Claim Element	ANVIL Mapping	Risk Assessment
Confirming presence of authorized helper at predefined intervals during treatment	ANVIL confirms prescriber presence continuously during telehealth session	**[YELLOW]** Conceptual parallel: periodic presence check
Biometric authentication including video camera monitoring	ANVIL uses 3D facial geometry via video stream	**[YELLOW]** Both use camera-based biometric verification
Auto-termination (failsafe mode) on presence loss	ANVIL auto-terminates session on prescriber absence	**[YELLOW]** Similar enforcement action
Specific to dialysis/extracorporeal blood treatment devices at physical treatment location	ANVIL operates on telehealth video stream, not physical medical device	**[GREEN]** Different apparatus, different field (remote vs. bedside)

Overall Assessment: YELLOW. Most structurally relevant patent. However, claims are tightly bound to physical medical treatment devices (dialysis machines) with physical-location presence verification. ANVIL verifies remote prescriber presence via video stream, not bedside helper presence via physical proximity. The claims require a “medical treatment component configured to perform dialysis” which ANVIL categorically does not include. Literal infringement: None. Doctrine of Equivalents: Low—different apparatus, different environment (remote video vs. bedside physical), different purpose (prescribing auth vs. treatment supervision).

3. TARGETED COMPANY ANALYSIS

3.1 PatientVerifi / VerifiNow

VerifiNow launched PatientVerifi in February 2024 as a patient identity verification solution for telehealth. Uses voice biometrics, facial recognition, and liveness detection. However: (a) it verifies patients, not prescribers; (b) no US patent was identified under US11756323 or any other number for PatientVerifi/VerifiNow in USPTO searches; (c) the product appears to be an integration of third-party biometric APIs, not patented technology. No blocking IP identified.

3.2 Veriff

Estonia-based identity verification focused on KYC/onboarding for fintech and crypto. Video-first verification with 1,000+ data points analyzed per session. No US patents found covering continuous session authentication in a telehealth prescriber context. Their IP appears focused on document verification speed and fraud detection during initial onboarding, not ongoing session monitoring.

3.3 1Kosmos

Decentralized identity wallet with FedRAMP High authorization. Focus on passwordless workforce authentication with biometric identity proofing. No patents identified covering continuous video-based prescriber attestation during telehealth. Their IP is in the distributed identity wallet and credential management space.

3.4 Socure

Predictive identity verification using 20,000+ data points via their ID+ Identity Graph. Their patents (US2023/0376xxx series) cover identity fraud detection and risk scoring at the KYC onboarding stage, not continuous session authentication. Acquired Effectiv for transaction monitoring. No blocking patents for ANVIL’s architecture.

3.5 ID.me

First US patent for real-time online identity verification was announced June 2023. Their technology focuses on one-time identity proofing for government services (VA, IRS, Social Security). No continuous authentication claims. No telehealth prescriber-specific IP. Not a blocking risk.

3.6 Teladoc / Amwell

Teladoc holds ~159 applications and 69 granted patents, primarily acquired through InTouch Technologies (telehealth carts, robots, digital scopes). Amwell holds ~82 applications and 33 granted patents covering consumer-provider matching and platform connectivity. The Teladoc-Amwell patent wars (2015–2022, settled July 2022) centered on telehealth hardware and platform patents, not biometric verification. Neither company holds patents on continuous prescriber biometric attestation for DEA compliance. No blocking IP identified.

3.7 FaceTec

30+ issued patents on 3D liveness detection and face matching. Their 3D FaceMap technology creates time-stamped, non-reusable liveness data. Risk: if ANVIL uses or licenses FaceTec’s SDK, their patents are non-blocking (covered by license). If ANVIL builds its own 3D liveness from scratch, FaceTec’s specific implementation patents on 3D FaceMap generation methods could be relevant. Design-around: use alternative 3D depth estimation methods (structured light, ToF) or license FaceTec/similar vendor technology.

3.8 iProov

Holds patents on “Flashmark” illumination technology—a controlled color light sequence reflected off the face to verify real-time presence. If ANVIL implements a similar challenge-response illumination method, iProov’s patents could apply. Design-around: ANVIL’s continuous polling approach (geometry comparison against enrolled template at intervals) does not require challenge-response illumination, avoiding this patent family.

3.9 BioID

Holds patents on motion-analysis-based liveness detection (optical flow to distinguish 2D from 3D objects) and challenge-response head-turn verification. Design-around: ANVIL’s approach of continuous 3D geometry matching against enrolled templates avoids BioID’s specific optical flow and challenge-response methods.

4. GAP ANALYSIS — NOVEL ELEMENTS FOR PROVISIONAL FILING

The following ANVIL features appear novel based on the prior art search and should be emphasized in the provisional patent claims:

ANVIL Feature	Closest Prior Art	Gap / Novelty
Continuous prescriber presence attestation tied to controlled substance prescription authorization	US 12,112,849 (dialysis helper presence); US 12,192,199 (generic session auth)	No prior art links biometric presence verification to prescription authorization authority. This is the core novel combination.
DEA-compliant cryptographic signing of biometric attestation session logs	21 CFR 1311 defines EPCS signing requirements; no patent claims this for session attestation	Cryptographic binding of biometric session attestation to DEA audit format is entirely novel. EPCS patents cover prescription signing, not session presence logs.
Auto-termination of telehealth session upon prescriber biometric presence loss	US 6,111,517 (expired: computer access revocation); US 12,112,849 (dialysis failsafe)	Auto-termination of a telehealth session (not computer access, not medical device) upon prescriber departure is unclaimed in active patents.
Dual-mode architecture: Integration Mode (EHR plugin) and Standalone Mode (USB/portable)	No prior art for dual-mode prescriber attestation device	Hardware-agnostic deployment as both EHR integration and standalone compliance device is novel.
3D facial geometry polling at isochronous intervals with embedding comparison against enrolled DEA-registered template	FaceTec (3D FaceMap for onboarding); US 12,192,199 (2D motion region monitoring)	Isochronous polling with embedding comparison (not onboarding snapshot) against a DEA-linked enrollment template is novel.

5. RISK STRATIFICATION SUMMARY

Risk	Patent	Assignee	Mitigation
[YELLOW]	US 12,192,199	Paravision	Use 3D geometry (not 2D motion regions). Implement absence-based termination (not motion-triggered re-auth). Emphasize DEA regulatory context in claims.
[YELLOW]	US 12,112,849	Fresenius	Claims require physical medical treatment device (dialysis). ANVIL is a video-stream software system. No apparatus overlap. Low DoE risk.
[YELLOW]	US 9,106,789	Global Tel*Link	Claims specific to correctional facility visitation with video defacing. Different field of use. No healthcare/prescriber claims.
[YELLOW]	FaceTec portfolio (30+ patents)	FaceTec	License FaceTec SDK for 3D liveness, or implement alternative depth estimation. SDK license covers patent use.
[YELLOW]	iProov Flashmark patents	iProov	Do not implement challenge-response illumination. ANVIL's continuous polling approach avoids this patent family.
[GREEN]	All others surveyed	Various	No blocking patents identified for ANVIL's integrated architecture.

6. DESIGN-AROUND RECOMMENDATIONS

6.1 Continuous Authentication Layer

To further distance from US 12,192,199 (Paravision):

• Use 3D facial geometry embeddings (depth maps, landmark vectors), not 2D motion-region sample extraction. The Paravision patent specifically claims extracting sample data from a “monitor region” of 2D video frames and generating motion data.

• Implement isochronous polling at fixed, deterministic intervals (aligned with ANVIL’s “Physics Over Code” thesis) rather than event-triggered re-authentication. This creates a fundamentally different temporal architecture.

• Terminate sessions on presence absence, not re-authenticate on motion anomaly. ANVIL’s enforcement action (session termination) differs from Paravision’s (re-authentication cycle).

6.2 Liveness Detection / Anti-Spoofing

To avoid FaceTec, iProov, and BioID patent claims:

• License a PAD vendor SDK (FaceTec, AWS Rekognition Face Liveness, or equivalent) rather than building proprietary liveness detection. License covers patent exposure.

• If building proprietary: avoid challenge-response illumination patterns (iProov Flashmark) and avoid FaceTec’s specific 3D FaceMap generation pipeline. Use alternative approaches such as structured light depth estimation, temporal consistency analysis across polling intervals, or multi-frame passive liveness.

6.3 Cryptographic Audit Trail

No blocking patents identified. Recommendations for maximum defensibility:

• Implement FIPS 140-2 validated cryptographic modules per 21 CFR 1311 requirements. This is regulatory compliance, not a patentable method.

• Bind biometric attestation events (not just Rx signing events) to the cryptographic log chain. This extends beyond EPCS requirements and creates novel IP.

• Use HMAC-SHA256 with per-session keys derived from prescriber credential, session timestamp, and DEA registration number. This specific binding methodology is unclaimed.

6.4 DEA-Specific Formatting

DEA audit log formatting requirements under 21 CFR 1311.150 are regulatory specifications, not patentable methods. ANVIL’s compliance with these formats cannot be blocked by patents. The novel element is generating these logs from continuous biometric attestation data (rather than discrete Rx signing events), which has no prior art.

7. PROVISIONAL FILING STRATEGY RECOMMENDATIONS

Based on this FTO analysis, the following claim strategy maximizes ANVIL's patent strength by claiming the novel intersection elements that no prior art covers:

7.1 Primary Independent Claims Should Cover:

• A system for continuous prescriber biometric presence attestation during telehealth consultations for controlled substance prescribing, comprising the four-element architecture (3D facial geometry polling, embedding matching against enrolled templates, cryptographic session log signing, auto-termination on presence loss).

• A method for binding biometric presence attestation events to DEA-compliant audit logs during a telehealth prescriber session.

• A dual-mode prescriber compliance device operable as both an EHR integration module and a standalone USB verification unit.

7.2 Dependent Claims Should Specify:

• Isochronous polling intervals (specific frequencies and timing parameters).

• 3D facial geometry embedding generation methods (specific to distinguishing from 2D prior art).

• Cryptographic binding of attestation events to DEA registration numbers and session identifiers.

• Session termination protocols triggered by absence thresholds (specific timing and escalation procedures).

• Integration with EPCS systems and PDMP databases.

8. METHODOLOGY & LIMITATIONS

This FTO analysis was conducted using:

• Google Patents (full-text search of US granted patents and published applications)

• USPTO Patent Public Search

• Justia Patents database

• CPC code searches: G06F21/32, H04N7/15, G06F21/316, G16H10/60, H04L9/3297

• Company-specific assignee searches for all nine targeted companies

• Keyword searches across all four technical vectors specified in the research prompt

IMPORTANT LIMITATIONS:

• This analysis is not a legal opinion and does not constitute legal advice. It is a research deliverable to inform patent strategy.

• FTO searches cannot guarantee completeness. Newly published applications (within 18 months of filing) are not yet searchable.

• Patent claim interpretation is ultimately a legal determination made by courts. Infringement risk assessments here are engineering-informed evaluations, not legal conclusions.

• Canadian patent searches were not exhaustively completed and should be performed separately if Canadian commercialization is planned.

• Patent maintenance fee status was not individually verified for all patents. Some patents listed as active may have lapsed.

• This analysis should be reviewed by qualified patent counsel before making final commercialization or filing decisions.

— END OF REPORT —