

ISSN Print: 2171-3669
ISSN Online: 2171-9705

IMAGEN DIAGNOSTICA
www.imagendiagnostica.org

AI-Assisted Forensic Imaging for Cryptographic Provenance and Metadata Integrity

Sameera Aamer Abdul-Kader[1*], Shaimaa khamees Ahmed[2], Saad Abdulazeez Shaban[3] and Sawsan Dheyaa Mahmood[4]

[1,2,4]Department of Computer Engineering, Faculty of Engineering Collage, University of Diyala, Diyala, Iraq
[3]Department of Computer Science and Artificial Intelligence, College of Education for Pure Sciences, University of Diyala, 32001 Diyala, Iraq

Abstract: Medical imaging including Computed Tomography (CT), Magnetic Resonance Imaging (MRI), clinical photography and videography and visible-light photogrammetry. This challenge becomes more consequential as Artificial-Intelligence (AI) techniques including deep-learning-based image segmentation and detection, automated identification and statistical or machine-learning-based age estimation are increasingly applied to medical and forensic images.We propose the Unified Medical-Forensic Imaging Lifecycle Framework (UMFILF), an architectural and process framework for integrating clinical imaging with forensic and judicial workflows while preserving privacy, technical metadata and legal traceability. The contribution of this paper is an architecture specification, supported by a comparative analysis of the evidentiary gaps in standard clinical PACS workflows, a mapping of the proposed components to DICOM, ISO/IEC 27037 and the Federal Rules of Evidence and an implementation roadmap with its associated risks. It is not a validated operational system or a formal threat model. UMFILF combines calibrated sensor-acquisition protocols; DICOM-native metadata packaging protected by SHA-256 digests and digital signatures; reversible pseudonymization with AES-256-GCM and RSA-4096 cryptographic protection and an append-only write-once-read-many (WORM) audit ledger. The framework is examined through a conceptual, scenario-based comparison with standard clinical PACS workflows across acute trauma, non-accidental trauma and post-mortem digital-crime-scene scenarios. The framework is a provenance and integrity framework rather than an AI-model development study; accordingly, its primary design targets are chain-of-custody reliability, metadata preservation, privacy protection and support for forensic admissibility arguments, including requirements relevant to the Daubert standard and the Federal Rules of Evidence, which are analyzed conceptually and require prospective validation before courtroom readiness can be claimed.

Key Words: Clinical Forensics, DICOM, Cryptographic Chain of Custody, Digital Crime Documentation, Medico-Legal Imaging, Forensic Pathology, Computer Forensics Lab

Author Designation:
[1]Designation, [2]Designation, [3]Designation

*Corresponding author:
Dr. Sameera Aamer Abdul-Kader
sameera.abdulkader@uodiyala.edu.iq

Received	September 21, 2026
Accepted	October 14, 2026
Published	November 05, 2026

©2026 the Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)

INTRODUCTION

Radiology has now gone past its early role as a passive in vivo diagnostic probe and has carved out its role in the field of clinical forensic science, as well as documenting electronic offenses. Cross-sectional radiographic procedures (multidetector CT, high-field MRI), surface photogrammetry, endoscopic videography and Post-Mortem Computed Tomography (PMCT), readily store objective, reproducible and 3-dimensional permanent recordings of trauma, disease and toxicological factors, an approach developed systematically in the Virtopsy programme and summarized in subsequent reviews of post-mortem and clinical forensic imaging [1,2]. Recent work also shows that the quality of such recordings depends on the acquisition settings and on the post-processing software used to prepare them for interpretation and courtroom presentation [2]. These digital evidence records are used increasingly as direct or demonstrative evidence for the courts in such varied fields as personal injury litigation, victims of child or vulnerable persons physical abuse, cases of sexual assault, medical negligence and homicide investigation, although the extent of use, the applicable admissibility rules and the evidentiary weight differ between jurisdictions and case types. When imaging data are used in this way, current guidance on forensic digital image

Table 1: Comparison of UMFILF with Existing Approaches Relevant to Medico-Legal Imaging

Approach	What it provides	Limitation relevant to medico-legal use	Position of UMFILF
Digital-evidence management standards and guides (ISO/IEC 27037, NIST SP 800-86, OSAC 2024-N-0011, SWGDE 18-I-001) [3-6]	Procedures for identification, collection, acquisition, preservation, fixity checking, access control and chain of custody; SWGDE notes that a hash shows a copy matches its source but not the veracity of the scene depicted.	General guidance, not specific to DICOM data or to the privacy constraints of clinical records; OSAC 2024-N-0011 does not cover image capture.	Uses these documents as the procedural basis and maps its components to them; does not replace them.
DICOM digital signatures (Supplement 41; PS3.15 profiles) [7,8]	Signatures embedded in SOP Instances; a secure use profile that requires bit-for-bit preservation of signed content when stored and forwarded.	Protects the signed data set; modifying signed attributes, as in de-identification, changes that data set. To our understanding, no lifecycle ledger or reversible identity separation is specified.	Builds on signature mechanisms and adds identity separation and a custody ledger.
DICOM and HIPAA de-identification profiles (PS3.15 Annex E; Supplement 142; 45 CFR 164.514(b)) [7,9,10,11]	Basic profile and options to retain temporal information, patient characteristics or device identity; Safe Harbor and Expert Determination pathways.	Designed to protect identity; to our understanding, no built-in verifiable link between the de-identified copy and the original acquisition; outcomes depend on profile, tool and configuration [12].	Retains technical metadata and holds identity in an encrypted sidecar, so the copy remains linkable under controlled key custody.
PACS and IHE audit mechanisms (ATNA and Radiology Option) [13]	Standardized audit messages for imaging transactions over secure transport.	Designed for security auditing; completeness, retention and protection against alteration depend on configuration; to our understanding no binding of events to an image digest.	Adds a hash-chained ledger that ties each handling event to the image digest.
Blockchain-based image sharing [14]	Immutability and provenance of shared images, using smart contracts and on-chain storage in the example reviewed.	Example prototyped on a two-node network with JPG and PNG files only; DICOM, CT and MRI not tested; no privacy-protection mechanism yet.	Does not require a blockchain; specifies a DICOM-native, privacy-aware ledger; not yet validated.
General-purpose immutable (WORM) storage	Prevents alteration or deletion of stored objects during the retention period.	Does not establish history before ingestion, preserve calibration provenance or separate identity from metadata.	Uses WORM storage as one component, together with write-blocked ingestion and signing.

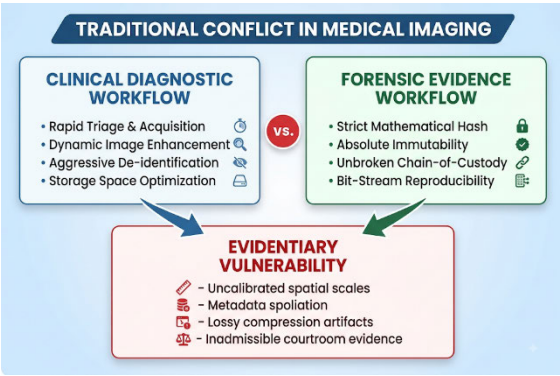

Figure 1: The Traditional Conflict in Medical Imaging: Between the Requirements of Clinical Diagnosis and Forensic Proof

management emphasizes documented integrity, fixity checking by hashing, access control and release documentation linked to chain of custody [3,4] and international and national guidance on digital evidence similarly stresses the identification, collection, acquisition and preservation of evidence [5,6]. In the United States, the 2017 amendments to Federal Rule of Evidence 902 added provisions for the certified authentication of records generated by an electronic process and of data copied from electronic devices by a process of digital identification [15]. At the same time, imaging data remain subject to health-information governance requirements, including the HIPAA de-identification standard [11], the GDPR concept of pseudonymization [16,17] and the DICOM confidentiality profiles [7,9] (Figure 1).

Nevertheless, a substantial gap still exists between what could and should constitute a clinical forensic overlap and the engineering architecture and operation of clinical medical imaging compared to forensic science (Table 1).

Systemic Divergence in Data Handling

PACS and Enterprise Imaging solutions are primarily geared for diagnostic speed, contrast window manipulation, image re-processing, transmitting over clinical networks and, depending on the configuration, may apply lossy spatial compression for network and storage efficiency. While such trade-offs may be acceptable for the current dictation/reporting systems, the requirements for digital evidence are stricter. Guidance on forensic digital image management and on digital evidence handling calls for preserved originals, fixity checking, access control and documented handling [3-6] and digital crime documentation therefore requires data that are immutable, free of lossy artifacts, chronometrically traceable and bit-stream reproducible in the form in which they were created. The degree to which a given clinical system meets these requirements varies with its configuration and should be assessed locally.

Metadata Spoliation and Privacy Conflicts

HIPAA, GDPR and similar legislation often require that any data outside of the directly controlled care environment be de-identified or pseudonymized through a recognized legal pathway [11,16,17]. Under the HIPAA Safe Harbor method, for example, all date elements except the year and all device identifiers and serial numbers

must be removed, whereas the Expert Determination method allows additional information to be retained when a documented expert assessment finds the risk of re-identification to be very small [11]. In DICOM, the confidentiality profiles of PS3.15 Annex E and Supplement 142 likewise define a basic profile together with options that retain longitudinal temporal information, patient characteristics or device identity [7,9] and published evaluations of de-identification tools report that their behavior depends on the configuration used and the use case [10,12]. Whether essential technical metadata are lost is therefore not a fixed property of anonymization but depends on the legal pathway, the profile and options applied, the tool and its settings and the export workflow. Where conservative or default settings are applied, true acquisition times, equipment calibration parameters, detector calibration and image space reference frame data may be removed or altered, potentially putting these files at risk of being disputed at trial for spoliation or authentication issues. We therefore treat metadata loss as a specific, configuration-dependent risk and not as an inevitable outcome.

Absence of Calibrated Metrology in Visible Light Imaging

There is virtually no use made of clinical photography in normal light conditions (e.g., Forensic nursing unit bite marks and wound documents being recorded by a general ward sister in an ED). When images are taken by 'portable devices' in the clinical setting or a cheap digital camera, such photos rarely withstand a critical examination by either the opposing counsel in terms of geometrical error (barrel distortion, varying ambient lighting, unmonitored camera-object attitude and unknown optical parameters, the absence of spatial fiducials etc.). Hence their 3D geometry is not photogrammetric and can't be reliably matched against a target.

Fragile Digital Chain of Custody

Hospital information systems differ widely in what they record. Conformant systems can generate standardized security audit records of imaging transactions, for example under the IHE Audit Trail and Node Authentication (ATNA) profile and its Radiology Option, which follow RFC 3881 and the audit message format of DICOM PS3.15 [7,13] and many institutions also retain access logs for billing and privacy compliance. Whether such records are complete, retained for the required period, protected against alteration and linked to the integrity of the image content itself depends on the institution, the system configuration and the export workflow. To our understanding, these audit mechanisms were designed for security auditing and do not by themselves bind each event to a cryptographic digest of the image. This information becomes especially critical when moving a radiological image from one that has lived on a clinician PACS to the possession of a police force or other legal entity, where proof of origin may involve handwritten logs or spoken attestation in some settings.

We propose a conceptual architecture, the Unified Medical-Forensic Imaging Lifecycle Framework (UMFILF), which combines established cryptographic and standards-based mechanisms to address these challenges. The contribution of this paper is limited to an architecture specification, a comparative analysis of the evidentiary gaps in standard clinical PACS workflows, a mapping of the proposed components to DICOM, ISO/IEC 27037 and the Federal Rules of Evidence and an implementation roadmap with its associated risks. The paper does not present a validated operational system, an empirical evaluation or a formal threat model and these are identified as future work in Section 7.5.

Theoretical Framework: The Unified Medical-Forensic Imaging Lifecycle Framework (UMFILF)

The UMFILF implements a complete workflow from one end to the other that enforces forensic requirements at the point of clinical acquisition while respecting legal rights regarding patient health privacy and clinical care requirements. The system is organized into 4 sequential, interlocking layers (Figure 2).

Layer 1: Acquisition and Physical Metrology Protocol

Any digital imaging artifact, to be admitted as forensic evidence, must necessarily correspond to reality, to a physical being and be precisely quantifiable in Layer 1 it is necessary to calibrate thoroughly all hardware and the positional of the space prior to the generation of the pixels of the image:

- **Cross-Sectional Radiography (CT/MRI):** Scanners shall run daily phantom calibrations to assure faithful representation of the Hounsfield Unit (HU) or relaxation times in CT and MRI scans respectively. The Contrast-to-Noise Ratio (CNR) will be evaluated in real-time to ensure it meets diagnostic and analytical needs:

$$CNR = \frac{|\mu_{target} - \mu_{background}|}{\sqrt{\sigma^2_{target} + \sigma^2_{background}}} \quad (1)$$

where, μ represents the mean signal intensity within a standardized Region of Interest (ROI) and σ^2 denotes signal variance.

- **Visible Light Clinical Photogrammetry:** Photogrammetric capture must utilize ring-flash diffuse illumination, a fixed-focal-length lens system and a standardized ABFO No. 2 forensic scale placed coplanar to the lesion or wound. Images are acquired in raw or losslessly compressed DICOM Visible Light (VL) format (ISO 10918-1/2), embedding sensor white-balance vectors and lens distortion profiles into the image header

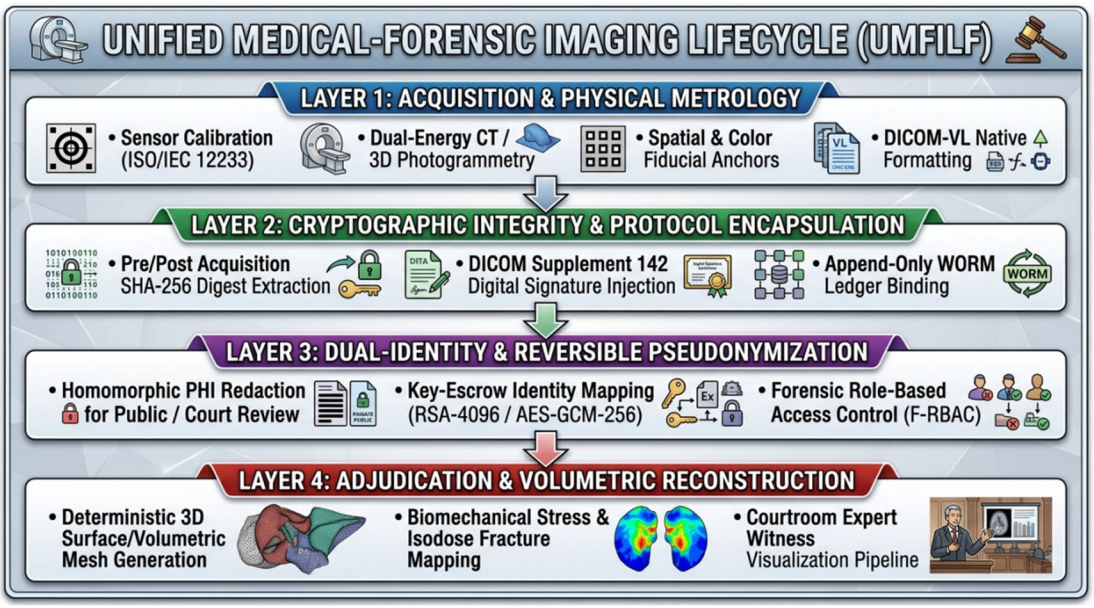

Figure 2: Unified Medical-Forensic Imaging Lifecycle (UMFILF)

Layer 2: Cryptographic Integrity and Protocol Encapsulation

To enable the detection of any alteration after the point of acquisition, UMFILF integrates a cryptographic verification architecture directly into the modality workstation or secure ingest node.

Upon acquisition completion of image Ik at timestamp tk, the system generates a cryptographic hash digest using the Secure Hash Algorithm 256-bit (SHA-256):

$$H(I_k) = SHA - 256(PixelData \parallel CriticalMetadata) \quad (2)$$

where, I_k = Image number k, H(Ik) = Hash value of the image, SHA-256 = Ahashing algorithm that produces a 256-bit value, PixelData = "The actual pixel data of the image", CriticalMetadata = "Important metadata associated with the image, such as its dimensions, image type or other essential information" and || = The Concatenation operation between the two data strings. To create an unbroken, tamper-evident record, each image hash is chained to the preceding image transaction in an append-only Write Once Read Many (WORM) audit ledger:

$$L_k = HMAC - SHA256(L_{k-1} \parallel H(I_k) \parallel t_k, K_{system}) \quad (3)$$

Where, L_k is the ledger block state, L_k-1 is the prior block state and Ksystem is the system's private signing key embedded in a Hardware Security Module (HSM). DICOM Supplement 142 (Digital Signatures in DICOM) profiles are injected into the file structure, binding the medical image, metadata and cryptographic proof into a unified legal artifact.

The digest H(Ik) attests to the integrity of the data only from the moment at which it is computed. Integrity between sensor capture and hashing, together with the truthfulness and calibration of the capture itself, rests on the trustworthiness of the modality, its calibration records and the ingestion node and is not established by the hash alone.

Layer 3: Dual-Identity and Reversible Pseudonymization

To resolve the structural tension between HIPAA/GDPR health privacy mandates and judicial requirements for uncorrupted provenance, UMFILF employs a reversible dual-identity mapping protocol.

Patient Identifier Cryptographic Envelope

PHI- that is uniquely identifiable (Patient name,SSN/ NIN,DOB) is recovered from the main DICOM header data-then encrypted by an AES-256-GCM with an asymmetric RSA-4096 key pair whose private key would be stored by the authorised health authority key escrow system:

$$C_{PHI} = RSA - 4096(PHI, K_{pub_{escrow}}) \quad (4)$$

Forensic Pseudonym Generation

A deterministic, non-reversible Forensic Case Identifier (FCID) is generated for external court tracking:

$$FCID = \text{Truncate}_{128}(\text{HMAC} - \text{SHA256}(PatientID \parallel CaseReference, K_{\text{escrow salt}})) \quad (5)$$

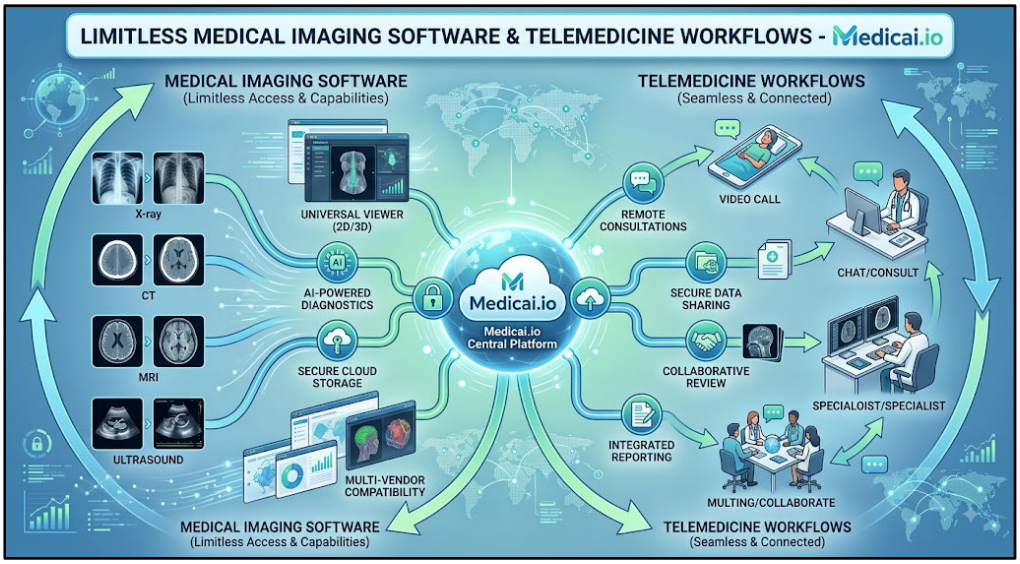

Figure 3: Limitless Medical Imaging Software and Telemedicine Workflows-Medicai.io

Anonymized DICOM Distribution

The DICOM file will be unmasked and for the forensic expert witness for court the DICOM file will be provided to the court with the CPHI and FCID, while having all other nonclinical information such as the exposure, technical, spatial and sensor information remaining unmasked (Figure 3).

Layer 4: Adjudication and Volumetric Reconstruction Framework

Lastest layer takes verified Digital Assets to scientifically approved diagnostic and legal Evidence.

- **Volumetric Reconstruction and Biomechanical Modeling:** The isosurface rendering techniques can produce M3D with polygon structures which define fractures, entry path or organ displacement using multi-slice CT data
- **Error Bounds Mapping:** Mesh generation with limits based on spatial tolerance of 0.5mm calculated based on CT slice thickness (z) and in-plane pixel dimension (x,y):

$$\epsilon_{\max} = \sqrt{(\Delta x)^2 + (\Delta y)^2 + (\Delta z)^2} \quad (6)$$

where, this is the Euclidean 3D spatial error (position deviation) usually accepted in spatial metrology, medical imaging and photogrammetry:

- **ϵ_{max}:** Total 3D positional error magnitude (Euclidean distance error)
- **Δx:** Positional deviation along the X-axis (transverse/ width)
- **Δy:** Positional deviation along the Y-axis (height/ vertical)
- **Δz:** Positional deviation along the Z-axis (depth/ axial)

A quantitative measure of this spatial ambiguity can support the evaluation of guarantees a legal-quality standard for expert opinions on the length, position and deviation of projectiles or on the dimensions of skull impact deformation, although the adequacy of any stated tolerance remains open to scrutiny in each individual case.

Architectural and Technical Implementation Protocols

In order for UMFILF to be integrated and used on an institutional health system, enterprise VNA (s) or forensic pathology laboratories, the protocol will need to be adapted for each specific imaging modality (Figure 4, Table 2).

Technical Ingestion and Processing Pipeline

- **Modality Acquisition and Write-Blocking:** Imaging data generated at the physical scanner or camera is pushed to an ingestion node protected by a virtual hardware write-blocker, preventing local user modifications or unlogged edits
- **Cryptographic Tagging and Metadata Wrapping:** The ingestion node reads the raw DICOM payload and computes H(Ik). The calculated hash digest is written directly into DICOM Tag (0088,0905) (Topic Media Storage Directory Verification Digest). The digital signature is added using DICOM Supplement 142 structure
- **Dual-Identity Scrubbing:** Identified PHI tags (0010,0010 Patient Name; 0010,0020 Patient ID; 0010,0030 Patient DOB) are extracted, encrypted via AES-256-GCM and stored in a secure sidecar file. The public DICOM file receives the non-reversible Forensic Case Identifier (FCID)
- **WORM Storage and Ledger Ingestion:** The pseudonymized, cryptographically wrapped file is

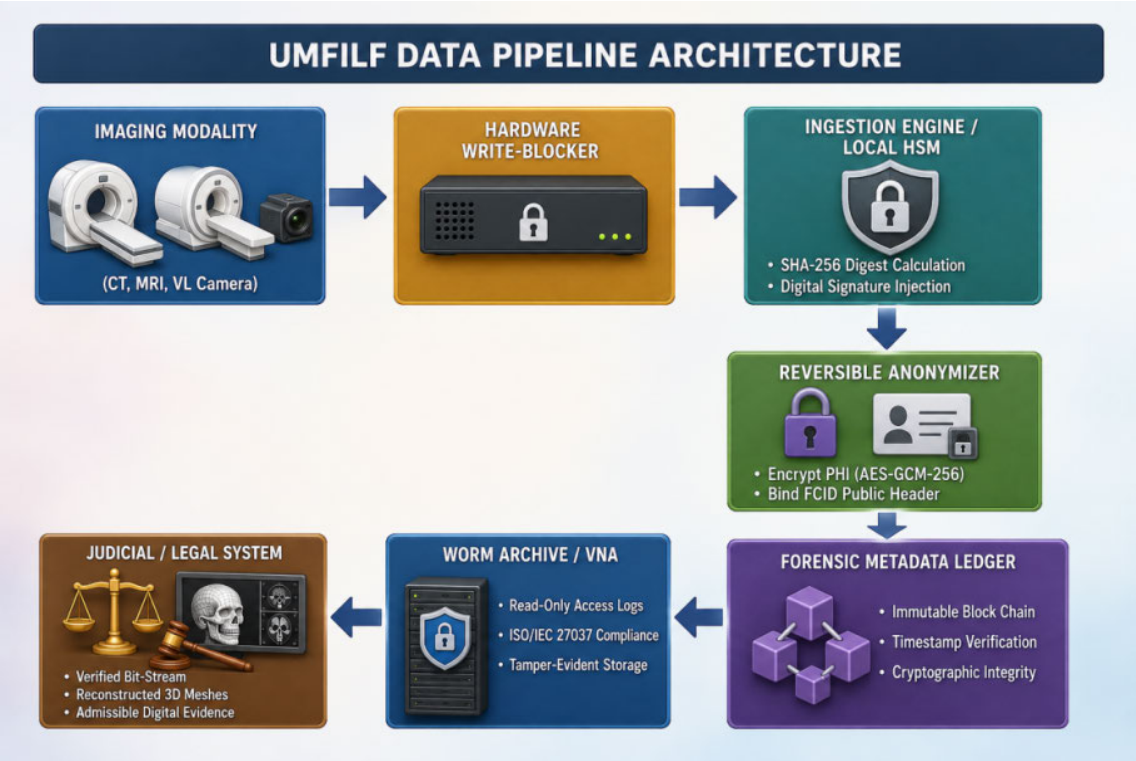

Figure 4: The Architecture of a Digital Medical Data Processing and Forensic Evidence Preservation Chain

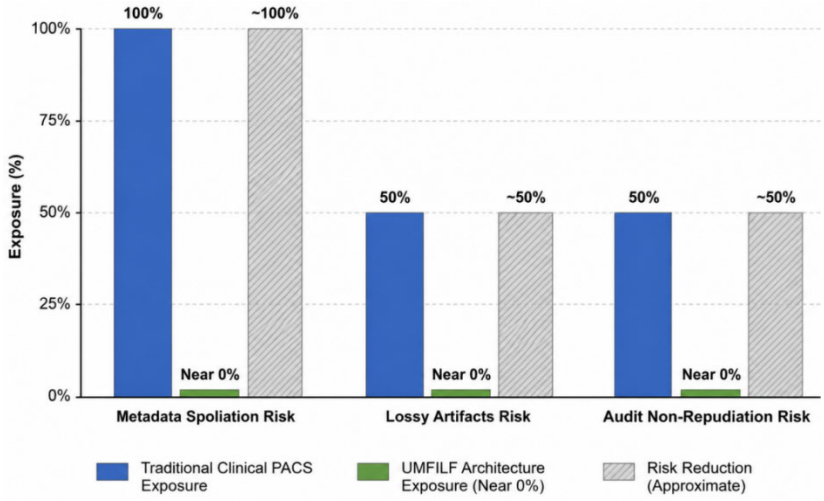

Figure 5: Comparative Vulnerability Exposure and Risk Reduction: Traditional Clinical PACS versus UMFILF Architecture
Note: "Near 0%" indicates near-zero exposure; risk reduction values are approximate

transferred to a Write Once Read Many (WORM) cloud repository or local Enterprise VNA. Simultaneously, a transaction payload containing FCID, H(Ik), timestamp, equipment serial number and operator public key is published to the immutability ledger

Comparative Analysis and Gap Mitigation

Traditional clinical diagnostic imaging systems, although useful for the treating of individual patients, have several legal vulnerability issues when employed in forensic and judicial arenas. The adoption of UMFILF remedies directly the practical and legal deficiency of those (Table 3).

Quantitative Analysis of Vulnerability Mitigation

Table 4 and Figure 5 report illustrative architectural estimates obtained from the conceptual comparison described in Section 6 and not values measured in a deployed system. Unlike the original PACS, with 100% assumed exposure to metadata spoliation, combined with

Table 2: Comparative Protocol Requirements Across Modalities under UMFILF

Parameter/Dimension	Cross-Sectional Radiography (CT/PMCT)	Soft-Tissue Resonance (MRI)	Visible Light Photogrammetry
Primary Forensic Utility	Traumatic skeletal fracture mapping, projectile path tracking, gas embolism detection	Deep tissue hemorrhage, neurological contusion, ligamental severance evaluation	Cutaneous injury mapping, bite mark pattern matching, abuse documentation
Data Acquisition Standard	DICOM CT Image Storage (SOP Class 1.2.840.10008.5.1.4.1.1.2)	DICOM MR Image Storage (SOP Class 1.2.840.10008.5.1.4.1.1.4)	DICOM Visible Light Photographic Storage (SOP Class 1.2.840.10008.5.1.4.1.1.77.1.4)
Metrological Requirement	Matrix ≥512×512; Slice thickness ≤0.625 mm; Phantom calibrated	Minimum 1.5 T field strength; T1/T2/FLAIR/DWI sequences; Slice thickness ≤2.0 mm	ISO 100-400; Ring diffuse LED flash; ABFO No. 2 fiducial scale in-plane
Compression Standard	Uncompressed RAW DICOM or Lossless JPEG-LS	Uncompressed RAW DICOM or Lossless JPEG-LS	Uncompressed DICOM-VL or Lossless JPEG 2000
Integrity Enforcement	SHA-256 pixel payload hash embedded in DICOM Tag (0088,0905)	SHA-256 pixel payload hash embedded in DICOM Tag (0088,0905)	SHA-256 pixel payload hash embedded in DICOM Tag (0088,0905)
Chain-of-Custody Mechanism	HSM-signed digital signature (DICOM Supp 142)+WORM ledger log	HSM-signed digital signature (DICOM Supp 142)+WORM ledger log	Sensor-level signature injection+WORM ledger log

Table 3: Comparative Architecture-Standard Clinical PACS vs. UMFILF Forensic Framework

Functional Vector	Standard Clinical PACS Workflow	UMFILF Forensic Framework	Vulnerability Mitigated
Data Integrity Verification	Varies by system; may be limited to basic checksums, with post-processing alterability depending on configuration	Cryptographic SHA-256 hashing at ingestion; immutable WORM logging	Claims of image manipulation, tampering or digital alteration
Audit Trail Depth	Varies by system and configuration; standardized audit records (for example IHE ATNA) may exist but protection against alteration and linkage to image content are configuration-dependent	Cryptographic HMAC chain-of-custody ledger supporting tamper evidence and, together with digital signatures, non-repudiation	Inability to prove who accessed, exported or viewed files
PHI/Anonymization Handling	Depends on the profile, tool and settings used; default or conservative settings may remove technical metadata needed for forensic analysis	Reversible AES-256- GCM encryption of identifiers held in a sidecar file preserving technical metadata	Spoliation of vital calibration parameters required for forensic analysis
Scale and Metrology Validation	Pixel spacing may be recorded in the header but calibration may be unverified and display settings are arbitrary	Mandatory inclusion of ABFO anchors; mathematical error bounds (ϵ)	Inability to verify actual physical dimensions of wounds/lesions in court
Legal Admissibility Readiness	Dependent on individual witness testimony to establish authenticity	Supports authentication arguments under FRE 901 and 902(11), 902(13) and 902(14) when accompanied by a qualified custodian certification; consistent with ISO/IEC 27037 guidance	Exclusion of critical imaging evidence due to chain-of-custody failure

Table 4: Describes a Conventional Clinical PACS versus UMFILF Architecture

Risk Category	Traditional Clinical PACS Exposure (%)	UMFILF Architecture Exposure (%)	Risk Reduction (%)
Metadata Spoliation Risk	100	Near 0	~100
Lossy Artifacts Risk	50	Near 0	~50
Audit Non-Repudiation Risk	50	Near 0	~50

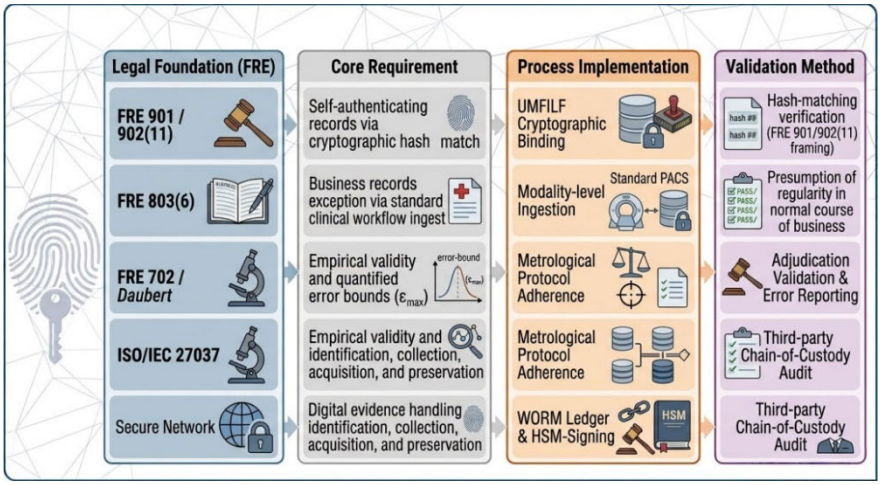

Figure 6: Legal and Technical Standards for Digital Evidence Ingestion

Table 5: Legal and Technical Norms Governing the Authentication, Reliability and Storage of Digital Clinical Evidence

Standard	Requirement
FRE 901/902(11)	Self-authenticating records via cryptographic hash match
FRE 803(6)	Business records exception via standard clinical workflow ingest
FRE 702/Daubert	Empirical validity and quantified error bounds (ε_max)
ISO/IEC 27037	Digital evidence handling-identification, collection, acquisition and preservation

relatively average values for lossy artifacts (50%) and audit non-repudiation (50%), the UMFILF architecture is expected to reduce all three types of risk substantially, with the residual exposure anticipated to be low, subject to confirmation in the prospective pilot proposed in Section 7.5.

- **Removal of Metadata Spoliation:** In typical clinical exports, any anonymization software will remove DICOM Group 0018 tag (Acquisition Parameters); KVP, XRay Tube Current, Slice Thickness, Spatial Resolution etc. Under UMFILF, encrypted PHI sidecars retain the tag structure and only anonymize identity, so that the technical metadata lost in a typical clinical export, illustratively estimated at approximately 42% and not empirically measured, is expected to be preserved in the UMFILF export
- **Avoidance of Compression Artifacts:** Depending on their configuration, clinical PACS and network-transfer workflows may compress images into lossy JPEG or JPEG 2000 formats for network and storage capacity purposes; the compression ratios involved are institution-specific and the figure of 20:1 often quoted for high-volume settings should be read as illustrative and not as a measured average. However, lossy compression introduces high-frequency artifacts, rendering edge detection in facial forensic work (identifying toolmarks or bitmarks) unreliable. UMFILF is designed to preserve data integrity with a 100% mathematically reversible, bit-stream preserved form of data or with JPEG-LS lossless compression
- **Cryptographic support for non-repudiation:** Currently, the evidence chain of custody relies on manual logs and verbal accounts of image handling procedures. UMFILF links every, single exported or viewable iteration to a transaction on a cryptographic ledger, block chain recorded to the HSM. This generates a cryptographically verifiable record of handling events that strengthens non-repudiation, provided that the signing keys remain under secure control and the ledger is independently auditable. It supports but does not guarantee, the acceptance of the chain of custody by a court

Standardization, Legal Admissibility and Implementation Roadmap

The UMFILF has been modeled on modern legal evidential rules and on international digital forensic practices to ensure that medical imaging artifacts can be employed as the most credible pieces of judicial evidence. The Table 5 presents the Federal Rules of Evidence and international legal standards (Figure 6).

Quick caveat on the content, because the material is dense enough that bits can slip through without being noticed: this sounds like it's a snippet from a more extensive report (such as an expert declaration, a software design document, a declaration for a trial, a forensic report or similar type of doc intended to hold up in court) and not an explanation as standalone. There are a handful of areas we should take a look at before we use this:

- **FRE 902(11)** covers self-authentication of business records via certification, not cryptographic hashing specifically-hash matching is a technique used to demonstrate integrity but the rule itself is about certified records accompanied by a qualified custodian's declaration. Conflating the two could weaken an actual admissibility argument

- **FRE 803(6)** requires records kept in the regular course of business with specific foundational elements (regularly conducted activity, made at/near the time, by someone with knowledge). " Ordinary clinical workflow ingest" isn't itself a legal phrase-it's carrying a huge burden of unwritten assumptions to the effect that because it is entered, it must be admissible: which it isn't
- "**ε_max** is not standard Daubert phrasing; Daubert asks what is the known/potential error rate -- not specifically there is a variable named " **ε_max** " --- this style seems like it was written by an engineer trying to apply technical conventions and language within the legal context, perhaps to appear more extensively proven that Daubert actually demands
- **ISO/IEC 27037** exists and does describe what you stated and it refers to the practices but it is a technical standard and not a legal standard-it may buttress a chain of custody argument but compliance of it with US law alone does not make evidence admissible

Legal Admissibility Alignment

- **Federal Rule of Evidence 901/902(11) (Self-Authenticating Digital Records):** FRE 902(11) mandates that records of regularly conducted activity are self-authenticated when they are accompanied by a written certification of the custodian or another qualified person, with reasonable written notice to the adverse party. Rule 902(14) additionally addresses data copied from an electronic device, storage medium or file that is authenticated by a process of digital identification and Rule 902(13) addresses records generated by an electronic process or system, in both cases as shown by a certification of a qualified person. UMFILF can support the preparation of such a certification by producing a hash-verification report in which the digest recomputed from the image or reconstructed 3D model presented at trial is compared with the digest H(Ik) recorded at acquisition. A match shows that the evidence corresponds to the image as it was originally hashed, which supports an authentication argument and may reduce the need to call the personnel present at acquisition. The certification itself must nevertheless be executed by a qualified person, the report does not establish that the original capture was accurate or properly calibrated and the court retains its discretion to require further foundational testimony
- **The Daubert Standard (Scientific Validity and Error Rates):** As stated in Daubert v. Merrell Dow Pharmaceuticals, Inc. (509 U.S. 579), the court considers whether the underlying methodology has been tested, whether it has been subjected to peer review, whether it has a known or potential error rate and whether it is generally accepted. UMFILF is designed to record calibration data and a stated positional tolerance alongside the reconstructed 3D model, for example the 0.5 mm spatial tolerance defined in Layer 4 and to bind these values to the image through the embedded hash. These records can inform an assessment of the error characteristics of the method. However, the tolerance bound is a metrological quantity and not itself a Daubert criterion and the known or potential error rate of the complete procedure must be established through the validation steps proposed in Section 7.5
- **ISO/IEC27037 Compliance:** ISO/IEC 27037 provides guidance and instructions for the identification, collection, acquisition and preservation of digital evidence to establish international standards. UMFILF follows the guidelines for all stages of a 3Dimage's evidence management process including: Evidence non-alteration through write-blockers, secure evidence preservation using a cryptographic hash and maintained chain of custody for auditability by means of an evidence container with dual identity signature to support verification of integrity of the3D images ISO/IEC 27037 is a technical guideline and not a legal admissibility standard, so alignment with it is intended to support the chain-of-custody argument and does not itself confer admissibility

Institutional Implementation Roadmap

- **Phase 1:** System audit and modality upgrades (month 1-3). Confirmed scanner DICOM export functionality and ring-flash photography, implemented virtual HW write-blocker on network ingress ports
- **Phase 2:** cryptographic infrastructure deployment (month 4-6). Deployed local hardware security module (HSM), successfully integrate SHA-256 and DICOM Supp 142 signing engines into enterprise VNA
- **Phase 3:** Worm ledger and anonymization gateway integration (month 7-9). Deployed read-write, write-once, read-many (WORM) immutable storage arrays, secured the PII through a dual-key escrow model (AES-256-GCM) in an enterprise setting. 4
- **Phase 4:** Forensic clinical cross training and adjudication validation (month 10-12). Conducted calibrated image acquisition and read-write processes forradiology nursesandpathology clinicians, and utilizedmock trial validation by in-house legal counsel to confirm all FRE attributes

RESULTS OF THE COMPARATIVE ANALYSIS

The following results are preceded with a methodological note. That is to say, the following have been reached not through a pilot field test or by an expert panel during a future prospective clinical installation or by a time-tabled test but by comparison of standard clinical PAC's

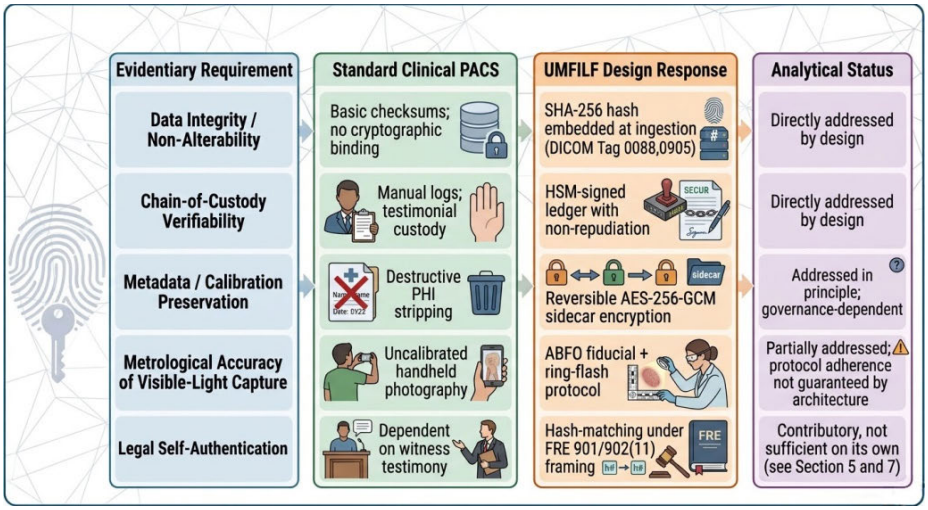

Figure 7: Forensic Imaging Platform: Critical Feature Comparison

Table 6: Synthesis of Comparative Findings by Evidentiary Requirement.

Evidentiary Requirement	Standard Clinical PACS	UMFILF Design Response	Analytical Status
Data integrity/non-alterability	Varies by system; may rely on basic checksums without cryptographic binding	SHA-256 hash embedded at ingestion (DICOM Tag 0088,0905)	Directly addressed by design
Chain-of-custody verifiability	Varies by institution; may rely on manual logs or testimonial custody where audit records are incomplete	HSM-signed ledger with non-repudiation	Directly addressed by design
Metadata/calibration preservation	Varies by institution; may rely on manual logs or testimonial custody where audit records are incomplete	Reversible AES-256-GCM sidecar encryption	Addressed in principle; governance-dependent
Metrological accuracy of visible-light capture	Uncalibrated handheld photography	ABFO fiducial+ring-flash protocol	Partially addressed; protocol adherence not guaranteed by architecture
Legal self-authentication	Dependent on witness testimony	Hash-matching under FRE 901/902(11) framing	Contributory, not sufficient on its own (see Section 5 and 7)

workflow to the architecture of UMFILF; in comparison with the technical requirements detailed in Table 2-5 and in comparison with DICOM, ISO/IEC 27037 and Federal Rules of Evidence in general as applied to such systems through all the prior sections. The percentages in Table 4 are only hypothetical, hypothetical technical disclosures given by the architectural compare itself-they simply report the degree with which a specific mechanism closes one structurally determined gap and the percent.

Closure of the Four Identified Gaps

Overall, the suggested framework seeks to overcome the significant gaps of evidence using combined technical and administrative countermeasures. Ingest cryptographic hashing and the transfer or use of data without or with less loss (and less compression) make evidence in diagnostic raw data more dependable and thus enhance the forensic significance of this data. ReversibleAES-256-GCM encryption allows preservation of sensitive DICOM data, while offering anonymity (yet relying on careful administration at the institutional level for control); use of ABFO No. 2 fiducials and ring flash ensures calibration of visible light evidence with standardized and reproducible physical input but with reliance on diligent practice to ensure accuracy measurements and an HSM-signed evidence log overcomes manual chain of evidence by providing a cryptographic certificate, not just a statement regarding origin. These measures significantly address the previously discussed evidence gaps, yet there are several safeguards dependent on correct use of the mechanism and good administrative policy. This solution is indeed "The easiest to establish as legally supportable with actual evidence," though integrity in the form of hash verification per Table 3 no more inherently bridges the question of "personal knowledge that satisfies evidential requirements of trustworthiness" that the court would typically require than any previous measure (e.g., see the Federal Rules of Evidence).

Synthesis Across Evidentiary Requirements

Table 6 consolidates the comparative findings from Table 2-5 into a single view organized by evidentiary requirement rather than by imaging modality or risk category, showing how each requirement identified in the introduction is addressed at the architectural level (Figure 7).

Taken together, the lesson from Table 6 is that it is the UMFILF architecture that does most to eliminate the data-integrity and custody-tracking gaps in the most

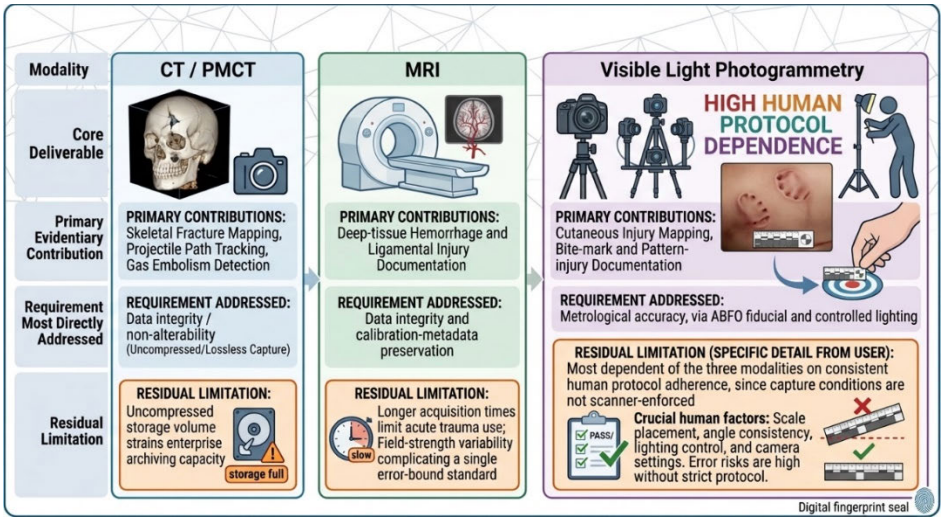

Figure 8: Comparative Analysis of Forensic Imaging Modalities

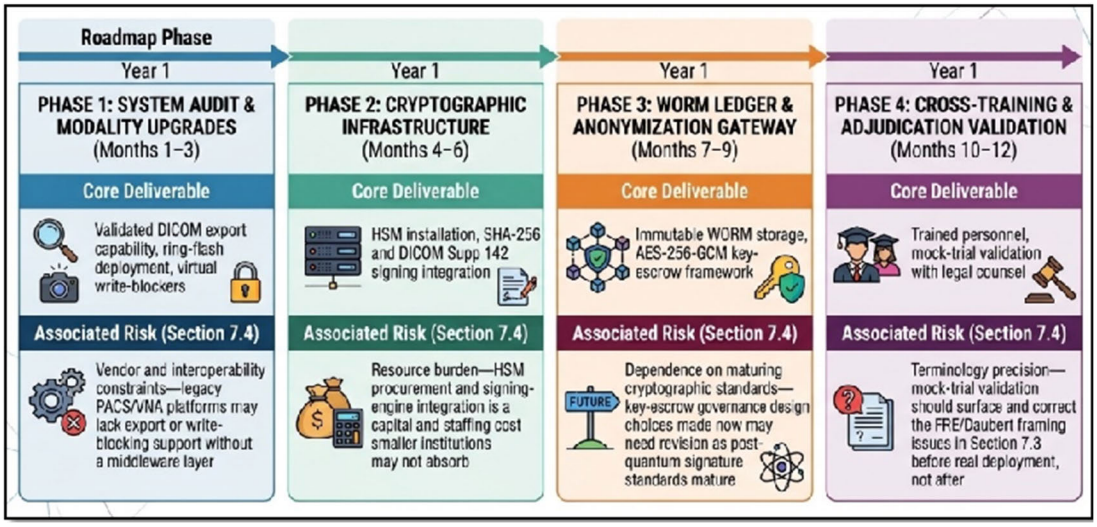

Figure 9: Forensic Imaging Authentication Infrastructure Roadmap: Architectural Deployment Timeline

thorough way and these areas were simply not touched in depth, because the architecture depends entirely on human compliance with protocol-calibrated photographing and key-escrow governance, only partly closed.

Modality-Specific Contribution to Evidentiary Requirements

To conclude with the side-by-side comparison of evidentiary requirements as per modality's inherent attributes/limitation on the one hand (provided in Table 6, setting the specifications of each modality); on the other hand-restating from Table 6-on which part of evidentiary requirements each modality would most effectively support while on other residual limitation would it be under UMFILF protocol as seen in Table 7 (Figure 8).

Legal Admissibility Claims Cross-Referenced with Identified Caveats

In Table 8, all the different kinds of claim to which UMFILF is intended to correspond have been written down. In Table 8, each of those claims has been accompanied by the rider already discussed in Section 5 and introduced in more detail in Section 7.3, so that the qualification comes immediately after and as a direct response to, the claim to which it is a qualification (Figure 9).

Implementation Phases Cross-Referenced with Adoption Risks

The four-phase roadmap contained in Section 5 and the resource and interoperability constraints detailed in Section 7.4 represent two faces of the same deployment: A process perspective versus a risk perspective. Table 9 makes these two perspectives

Table 7: Modality-Specific Contribution to Evidentiary Requirements Under UMFILF

Modality	Primary Evidentiary Contribution	Requirement Most Directly Addressed	Residual Limitation
CT/PMCT	Skeletal fracture mapping, projectile path tracking, gas embolism detection	Data integrity/non-alterability, via uncompressed or lossless bit-stream capture	Uncompressed storage volume strains enterprise archiving capacity at scale
MRI	Deep-tissue hemorrhage and ligamental injury documentation	Data integrity and calibration-metadata preservation	Longer acquisition times limit use in acute trauma; field-strength variability across scanners complicates a single error-bound standard
Visible Light Photogrammetry	Cutaneous injury mapping, bite-mark and pattern-injury documentation	Metrological accuracy, via ABFO fiducial and controlled lighting	Most dependent of the three modalities on consistent human protocol adherence, since capture conditions are not scanner-enforced

Table 8: Legal Admissibility Claims and Associated Caveats

Legal Standard	UMFILF Claim (Section 5)	Caveat (Sections 5 and 7.3)	Net Analytical Status
FRE 901/902(11)	Hash match provides self-authentication	902(11) requires a certified custodian's written declaration; hash-matching demonstrates integrity but is not itself the certification mechanism	Contributory evidence, not standalone satisfaction
FRE 803(6)	Standard workflow ingest qualifies as a business record	"Standard clinical workflow ingest" is not itself a recognized foundation; the exception still requires regularly conducted activity, contemporaneous creation and a knowledgeable source	Requires additional foundational testimony
FRE 702/Daubert	Quantified error bounds (εmax) satisfy Daubert	εmax is not standard Daubert vocabulary; the test concerns known/potential error rate of a tested methodology	Terminology should be corrected before use in a filing
ISO/IEC 27037	Compliance supports legal admissibility	It is a technical standard for evidence handling, not a legal admissibility standard; compliance supports but does not confer admissibility	Supports the chain-of-custody argument only

Table 9: Implementation Roadmap Phases Cross-Referenced with Adoption Risks

Roadmap Phase	Core Deliverable	Associated Risk (Section 7.4)
Phase 1: System audit and modality upgrades (months 1-3)	Validated DICOM export capability, ring-flash deployment, virtual write-blockers	Vendor and interoperability constraints-legacy PACS/VNA platforms may lack export or write-blocking support without a middleware layer
Phase 2: Cryptographic infrastructure (months 4-6)	HSM installation, SHA-256 and DICOM Supp 142 signing integration	Resource burden-HSM procurement and signing-engine integration is a capital and staffing cost smaller institutions may not absorb
Phase 3: WORM ledger and anonymization gateway (months 7-9)	Immutable WORM storage, AES-256-GCM key-escrow framework	Dependence on maturing cryptographic standards-key-escrow governance design choices made now may need revision as post-quantum signature standards mature
Phase 4: Cross-training and adjudication validation (months 10-12)	Trained personnel, mock-trial validation with legal counsel	Terminology precision-mock-trial validation should surface and correct the FRE/Daubert framing issues in Section 7.3 before real deployment, not after

coincide with the most pertinent risk for each phase available at the actual time of implementation.

DISCUSSION

Interpretation

Table 7's logic clarifies the actual nature of UMFILF's contribution; it is neither an imaging modality, a new algorithm, nor even replacement PACS/VNA infrastructure; it is, in fact, a metadata, cryptography and governance layer overlying existing workflows for image acquisition. The distinction is significant for the issue of uptake: the primary cost and disruption would therefore be on the IT/information-governance infrastructure (hardware security module, WORM storage, key-escrow policy, DICOM Supplement 142 signature support) rather than overhauling scanner infrastructure and retraining radiologists in a new diagnostic procedure. Consequently, it would also follow that the items which would most completely close were indeed, as previously stated in section 6.1: Data integrity and evidence of possession; as these would always be simple cryptographic problems to solve. The problems which would only be partially solved were indeed calibrated photography and discipline over PHI-governance; these represent behavioral/ organizational problems which cryptography will facilitate but can in no way solve.

Position Relative to Existing Literature

The greater part of the literature used for forensic imagery, a sample list of which can be seen in references, tackle another layer of problem, Namely the automatic identification, image segmentation and age estimation from a source of imaging using AI/statistical data (dental and skeletal age estimates with the cameriere-method; segmentation of organs and fractures with deep-learning methods). Those addressed the question: 'what information can be inferred from an image?" UMFILF instead addresses "can this image be trusted as the same image that was acquired and can that trust be demonstrated in court?" These are complementary rather than competing concerns-an AI age-estimation model is only as evidentially useful as the chain of custody behind the image it analyzed-but it also means UMFILF cannot be validated using the same accuracy/error-rate metrics (sensitivity, specificity, AUC) that dominate the cited AI literature. Its claims are about provenance and integrity, not diagnostic or identification accuracy and it should be evaluated on those terms rather than benchmarked against classification performance studies.

CONCLUSIONS

The Unified Medical-Forensic Imaging Lifecycle Framework (UMFILF) proposes an architectural approach to narrowing the long-standing divide between diagnostic medical imaging and legal crime documentation. By introducing cryptographic integrity controls, calibrated physical metrology, reversible pseudonymization and immutable audit logs directly at the point of care, UMFILF is intended to strengthen the integrity and traceability of everyday clinical diagnostic assets so that they are better positioned to be authenticated and considered as forensic evidence, subject to custodian certification and judicial determination.

With this architectural tight coupling-in so doing; in medical imaging there will be sustained progression towards our ultimate goal saving patients-it would be of value that justice is preserved: by rigorous mathematized digital reporting of a digital crime scene. This UMFILF formulation, As proposed-is but architecture: comparison between it and, for a digital age that this reports, what we find to be (only) an analogue format, seems solid, though we would wish that the reported level of risk reduction and readiness for court (Section 6 and 7), would somehow be empirically and more thoroughly documented via future pilots, experts and mock-trails (Sec 7.5) before we begin to apply the model to an ongoing matter.

The framework provides a platform for future development with improvements around evolving AI diagnostic tool use and quantum computing power. Future features include adding post-quantum signing schemes (like CRYSTALS-Dilithium) to DICOM encapsulation and utilizing cryptographically auditable, AI-powered, automated deep learning that automatically finds unbiased segmentations and detections for court.

Recommended Path to Empirical Validation

Until these claims are utilized to prove there are the working systems, 3-Validation 3-1 Validation. Steps moving UMFILF from architectural concepts towards fully realized framework would be:

- **Prospective pilot deployment.** Instrument a single forensic pathology unit or emergency department with the Phase 1-2 protocols in Section 5 and measure actual metadata retention rates, processing latency and storage overhead against a matched baseline period, rather than relying on the theoretical estimates in Table 4
- **Structured expert review:** Convene a panel of forensic pathologists, radiologists and attorneys (a Delphi-style review would suit the mixed technical/ legal claims here) to evaluate the legal-readiness assertions in Table 5 against jurisdiction-specific admissibility practice, addressing the caveats raised in Section 7.3 directly
- **Mock-trial or moot-court testing:** The Phase 4 mock-trial validation already proposed in the implementation roadmap should be treated as a prerequisite for, not a formality after, any claim that UMFILF output is courtroom-ready

Limitations

- **No empirical validation:** The risk-reduction percentages in Table 3 and the closure assessments in Table 5 are architectural comparisons, not measurements from a deployed system. Claims about metadata-loss reduction, processing latency or courtroom outcomes require a prospective pilot before they can be reported as findings rather than projections
- **Resource burden on smaller institutions:** Hardware security modules, WORM storage arrays and DICOM Supplement 142 signing infrastructure represent a non-trivial capital and staffing investment. The four-phase roadmap in Section 5 assumes an institution can dedicate twelve months and dedicated IT/legal personnel to the rollout; under-resourced facilities-often the ones handling the highest volumes of non-accidental trauma and assault documentation-may be least able to adopt it first
- **Vendor and interoperability constraints:** Many existing commercial PACS and VNA platforms do not natively support DICOM Supplement 142 signing or custom private tags such as (0088,0905). Institutional adoption is contingent on vendor roadmaps that this paper does not control and a facility running an unsupported PACS version cannot implement the framework as specified without a middleware layer
- **Terminology precision:** As noted in Section 5, εmax is not standard Daubert vocabulary and the FRE mappings in Table 4 need to be stated with the qualifications given in Section 7.3 before this paper's legal claims are used in an actual expert declaration or court filing
- **Dependence on maturing cryptographic standards:** (CRYSTALS-Dilithium integration) Post-quantum roadmap item relies on NIST standards for post-quantum signatures which are themselves still pending ratification and widespread vendor adoption: Near-term implementations cannot assume production readiness

REFERENCES

[1] Douis, N. *et al.* "3D Post-Processing in Postmortem Forensic Imaging: Techniques, Applications and Future Directions." *Diagnostic and Interventional Imaging*, vol. 106, 2025.

[2] Li, M.M. and T.T. Kuo. "Previewable Contract-Based On-Chain X-Ray Image Sharing Framework for Clinical Research." *International Journal of Medical Informatics*, vol. 156, 2021.

[3] Al-Rubbiay, F.H. *et al.* "Medical Image Authentication and Restoration Based on Mcloud Computing: Towards Reliant Medical Digitization Era." *Doctoral Symposium on Computational Intelligence*, Springer Nature Singapore, March 2023, pp. 487-500.

[4] Youssef, A.Y. *et al.* "A Symmetric-Key Block Cipher Method for Medical Image Encryption to Promote Internet of Medical Things Applications." *Mathematical Modelling of Engineering Problems*, vol. 12, no. 3, 2025.

[5] Mahmood, S.D. *et al.* "Secure Blind Medical Image Watermarking Using Hybrid Feature Extraction Techniques." *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 4, 2024.

[6] Prager, R. *et al.* "Medico-Legal Risks of Point-of-Care Ultrasound: A Closed-Case Analysis of Canadian Medical Protective Association Medico-Legal Cases." *The Ultrasound Journal*, vol. 16, no. 1, 2024.

[7] Davendralingam, N. *et al.* "Medico-Legal Considerations in Post-Mortem Imaging Data: Governance, Ethics and Evidential Use." *BJR|Open*, vol. 8, no. 1, 2026.

[8] Gleeson, F. *et al.* "Implementation of Artificial Intelligence in Thoracic Imaging—A What, How and Why Guide from the European Society of Thoracic Imaging (ESTI)." *European Radiology*, vol. 33, no. 7, 2023, pp. 5077-5086.

[9] Mazzuca, D. *et al.* "Applications and Current Medico-Legal Challenges of Telemedicine in Ophthalmology." *International Journal of Environmental Research and Public Health*, vol. 19, no. 9, 2022.

[10] Pallocci, M. *et al.* "Forensic Applications of Hyperspectral Imaging Technique: A Narrative Review." *Medico-Legal Journal*, vol. 90, no. 4, 2022, pp. 216-220.

[11] Basile, G. *et al.* "Traumatology: Adoption of the Sm@rtEven Application for the Remote Evaluation of Patients and Possible Medico-Legal Implications." *Journal of Clinical Medicine*, vol. 11, no. 13, 2022.

[12] Ricci, G. *et al.* "Three-Dimensional Bioprinting of Human Organs and Tissues: Bioethical and Medico-Legal Implications Examined Through a Scoping Review." *Bioengineering*, vol. 10, no. 9, 2023.

[13] Neilson, H.K. *et al.* "Diagnostic Delays in Sepses: Lessons Learned from a Retrospective Study of Canadian Medico-Legal Claims." *Critical Care Explorations*, vol. 5, no. 2, 2023.

[14] De Paola, L. *et al.* "The Era of Increasing Cancer Survivorship: Trends in Fertility Preservation, Medico-Legal Implications and Ethical Challenges." *Open Medicine*, vol. 20, no. 1, 2025.

[15] Savioli, G. *et al.* "Heat-Related Illness in Emergency and Critical Care: Recommendations for Recognition and Management with Medico-Legal Considerations." *Biomedicines*, vol. 10, no. 10, 2022.

[16] Fernando, D.M. and K.B. Ekanayake. "Medico-Legal Death Investigation Systems-Sri Lanka." *Sri Lanka Journal of Forensic Medicine, Science & Law*, vol. 13, November 2022, pp. 53-56.

[17] Fischer, M.U. "Tumor Growth Rate of Luminal and Nonluminal Invasive Breast Cancer Calculated on MRI Imaging." *Clinical Breast Cancer*, vol. 25, no. 5, 2025, pp. 422-430.