Date of first submission	2026-05-13
Date of acceptance of article for publication after review	2026-06-25
Date of publication/publication	2026-07-25

COMPLIANCE MANAGEMENT SYSTEMS IN OUTPATIENT COSMETIC CLINICS: INTEGRATING HIPAA, OSHA AND OPERATIONAL EXCELLENCE REQUIREMENTS

Kuzmichova Marharyta
Master`s Degree in Philology
Zhytomyr State University named after Franko
Corresponding author: marharyta_kuzmichova@ukr.net
ORCID: https://orcid.org/0009-0003-9639-5309

Abstract. *Outpatient aesthetic clinics in the United States find themselves in a rapidly evolving regulatory environment, yet compliance management practices at most small facilities have remained largely unchanged: documentation is updated once a year, training is conducted only when absolutely necessary, and compliance issues are addressed primarily in response to external risks. This article describes how the director of a clinic network, without a legal background, developed and implemented the Integrated Compliance Operations Framework (ICOF), a system that integrates HIPAA and OSHA compliance checks into the facility's daily operational processes rather than isolating them in a separate audit cycle. The data used in this study came from the Zenoti medical information system covering three operational years, as well as consultation protocols from an external specialist who verified that the identified risk areas align with the current enforcement priorities of federal regulatory agencies. Key elements of the developed system include a three-tiered authorization process for patient photographic documentation, a daily checklist for regulatory compliance checks, a four-factor analytical procedure for assessing potential violations, and a staff training program featuring practical simulations of real-life scenarios. The system has been implemented in four network locations and six external facilities. The results show that integrating regulatory checks into the facility's operational rhythm reduces actual risk more effectively than the traditional model of an annual compliance audit.*

Keywords: *compliance management, HIPAA, OSHA, aesthetic clinic, protection of patient medical information, operational standards, compliance audit.*

Introduction

The market for medical spas and outpatient aesthetic clinics in the U.S. is expanding rapidly: according to Grand View Research, the global market was valued at approximately $18.6 billion in 2023, with a projected compound annual growth rate of about 15% through 2030 [2]. The American Med Spa Association reports similar growth, with total industry revenue exceeding $5 billion [1]. At the same time, the regulatory burden is growing: outpatient aesthetic clinics are subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA), Occupational Safety and Health Administration (OSHA) standards, and additional state-level requirements. In Florida, federal requirements are supplemented by regulations from the State Medical Board and the Department of Health, which adds further complexity for small facility directors [7].

Most outpatient aesthetic clinics approach regulatory compliance reactively: documentation is updated once a year, training is conducted from time to time, and compliance is addressed mainly in response to external risk. Scientific and managerial literature on medical facility organization confirms that effective compliance is achieved only when checks are integrated into daily operations rather than maintained as a separate system [10].

According to IBM Security, the average cost of a single healthcare data breach in the U.S. in 2023 was $10.93 million, the highest of any industry for the thirteenth consecutive year [5]. For small healthcare facilities, the primary risk is not external cyberattacks but operational gaps: patient

ISSN: 2787-9364

photographs transmitted via unsecured personal phones, the absence of agreements with business partners and software vendors who have access to patients' medical information, and improper management of biohazardous materials [7]. All three risk categories are addressable through operational management.

Scientific publications on healthcare compliance management are aimed primarily at large medical networks with dedicated legal departments and budgets. How a director with operational experience but no legal training builds a system to comply with HIPAA and OSHA requirements in a small facility is virtually absent from the research.

The aim of this study is to describe the development and implementation of an integrated compliance management system within a network of outpatient aesthetic clinics, and to assess whether such a system can ensure regulatory compliance without increasing administrative burden.

The novelty of the approach lies not in the HIPAA and OSHA requirements themselves, which are externally established, but in integrating them into the clinic's daily operations so that each regulatory check coincides with an action the facility already performs.

Literature review

1. HIPAA in the Context of Small Healthcare Facilities

HIPAA, enacted in 1996 and significantly expanded by the 2003 Security Rule and the 2009 Health Information Technology for Economic and Clinical Health Act, establishes uniform standards for the protection of patients' health information for all healthcare facilities, including outpatient clinics [7; 12]. Academic research on HIPAA enforcement mechanisms has traditionally focused on large hospitals, while small outpatient facilities - which make up the majority of the sector - have been studied in far less detail [3].

Adler-Milstein and Jha found that incentives to transition to electronic health records increased the volume of patient medical information processed in outpatient settings without a proportional increase in resources to ensure its security in small facilities [3]. As a result, even a small clinic that maintains a patient database in a digital system and sends automated appointment reminders bears legal obligations under HIPAA that, just ten to fifteen years ago, were characteristic exclusively of large medical networks.

Among the categories of violations actively pursued by the U.S. Department of Health and Human Services' Office for Civil Rights in 2022–2023, three consistent priorities stand out: unauthorized disclosure of medical information via unsecured communication channels; the absence of agreements with business partners and technology service providers; and violations of patients' rights to access their own medical records [7]. Regarding the first and second categories, aesthetic clinics are particularly vulnerable due to the nature of their operations.

2. OSHA in the Context of Outpatient Aesthetic Facilities

The OSHA standard regarding bloodborne pathogens (29 CFR § 1910.1030) applies to all facilities where staff may come into contact with blood or potentially infectious materials, and aesthetic clinics performing injection and laser procedures unquestionably fall under this category [8]. At the same time, compliance with occupational safety requirements in small outpatient facilities remains one of the most neglected areas: documented annual staff training, a written plan for controlling exposure to biohazardous materials, and the recording of sharps injuries are often either absent or updated immediately prior to an anticipated inspection [8].

The absence of a written control plan at a facility where injection procedures are routinely performed is more than just a technical violation of regulations. In the event of a staff member being injured by a needle, the facility lacks an established protocol for responding, and the entire burden of responsibility falls on staff who have not been trained to handle such a situation.

3. A Culture of Compliance as an Operating System

Nilsen, in analyzing the theories and practices of implementing change in the healthcare system, found that the long-term adoption of a new approach depends primarily on whether staff understand its logic and perceive it as consistent with their own understanding of their role within the organization

ISSN: 2787-9364

[10]. Compliance checks presented to staff as an external legal burden provoke persistent defensive resistance. The same checks, presented as tools to protect patients and the staff themselves from legal consequences, are adopted without friction and carried out even in the absence of external oversight.

Braithwaite and his co-authors, studying the dynamics of organizational change in healthcare institutions, concluded that any management idea - regardless of its technical quality - requires systematic work to overcome cultural resistance in order to take root [9]. For the director of a small clinic without a dedicated compliance department, this means that compliance checks must be integrated into the very same routine rhythms of the facility that already exist and are followed: daily meetings, checklists, and inventory records.

4. Specific Compliance Challenges in Aesthetic Medicine

An aesthetic clinic operates within a regulatory framework that combines the requirements of a medical facility with the commercial realities of a business focused on attracting and retaining patients through marketing. Brandão and Ribeiro found that patient loyalty in aesthetic medicine is shaped in roughly equal measure by the quality of clinical work and the quality of service [11]. It is this duality that creates a specific regulatory tension: photographing patients before and after procedures is a necessary clinical tool and, at the same time, a potentially valuable marketing asset, which turns the management of photographic documentation into a constant source of risk in the absence of clearly established rules.

An analysis of statistics on medical information leaks confirms that in small healthcare facilities, such incidents occur primarily due to unauthorized actions by staff, rather than external attacks [5; 6]. The transfer of patient photographs via personal phones is usually not an intentional violation - it is a consequence of the absence of established procedures. Where procedures are established and their rationale is explained, staff behavior changes without coercion.

Materials and methods

1. Research Approach and Data Sources

The study is structured as a detailed case study comparing measured indicators before and after management intervention. This approach is commonly used to study complex organizational changes in real-world clinical settings, where controlled experiments are practically impossible and the number of institutions under study is limited [9; 10].

The primary study site is the Arviv Medical Aesthetics clinic in Miami, Florida. To verify the reproducibility of the developed system, branches of the network in Tampa, Ocala, and Coconut Creek were included in the analysis. Numerical and operational data were obtained from automatically generated reports of the Zenoti medical information system, which integrates medical records, appointment scheduling, billing, inventory management, and reporting. The system's automatic data generation eliminates errors associated with retrospective manual collection and enables independent auditing. Staff performance of daily operational tasks was tracked via the Prosp platform, which allowed the director to monitor the status of each branch remotely.

2. Study Author and Operational Context

The author of this study serves as Multi-Unit Facility Director of the Arviv Medical Aesthetics network and has no medical or legal education. This circumstance is important for evaluating the described changes: since the author lacks clinical and legal expertise, all improvements can be confidently attributed to management decisions rather than professional knowledge in related disciplines. Prior to working in medical aesthetics, the author managed a retail network at LVMH / Starboard Cruise Services for almost six years, where she gained experience managing operational systems that eliminate the human factor while ensuring compliance with standards. This experience shaped her approach to regulatory requirements: integrating compliance checks into operational processes using the same logic as inventory or personnel management, rather than treating them as a separate legal obligation.

2.1. Author's Contribution

This study introduces an original compliance architecture for outpatient aesthetic facilities, developed and implemented by the author around three methodological contributions. A risk-

ISSN: 2787-9364

prioritization model classifies compliance gaps along two dimensions - likelihood of occurrence and severity of legal and reputational consequences - so that remediation is sequenced rather than treated as an undifferentiated list of weaknesses. An operational integration methodology embeds regulatory checkpoints directly into the daily, weekly, and monthly workflows staff already perform, extending to the design of patient consent - a three-tiered authorization structure separating clinical, marketing, and educational use of photography - and to a four-factor procedure for determining whether a security incident triggers mandatory reporting. A parallel training model applies the same integration logic to staff development, embedding compliance competencies within the four-week new employee orientation rather than isolating them in a separate legal curriculum. The originality of the contribution lies not in the individual HIPAA and OSHA requirements, which are externally defined, but in the architecture that binds them to the facility's existing operational rhythm.

3. Status of Compliance Prior to the Changes

When the author assumed the Facility Director role in March 2024, the foundational compliance infrastructure was already in place. The facility had a designated compliance function, completed annual training, a maintained OSHA binder, and general staff awareness of confidentiality obligations. The facility was operating with a compliance baseline appropriate for its stage of development.

What the initial operational review identified was not a compliance violation - it was an integration gap. Compliance existed as a defined administrative function but had not yet been systematically embedded into daily operational workflows, individual performance accountability structures, or team culture. Annual training was completed, but compliance behaviors were not continuously reinforced between training events. The OSHA binder was maintained, but safety protocols had not been formally integrated into room turnover checklists and daily operational procedures. Compliance was understood as a shared organizational responsibility but was not measured as any individual staff member's specific accountability.

Compliance activities were conducted as separate administrative tasks disconnected from operational workflows. Annual training required approximately two to four hours per staff member per year. Ad hoc compliance responses were untracked and unmeasured. No daily compliance monitoring was in place, no task-tracking platform integration, no structured audit cycle. Compliance touchpoints were not embedded in daily workflow. As a result, compliance tasks were performed reactively when prompted rather than proactively as part of routine operations, and management time devoted to compliance was unstructured - estimated to involve significant untracked hours addressing compliance questions and gaps as they arose rather than preventing them systematically.

This gap - between compliance as an administrative obligation and compliance as an operational system - is the condition the Integrated Compliance Operations Framework was designed to address**.**

4. System Development Methodology

The development of the compliance management system proceeded along two parallel tracks: internal operational analysis and consultation with an external expert on healthcare regulatory compliance. The external expert was engaged specifically to answer three questions that could not be addressed through independent review of regulatory documents: which categories of violations are actively investigated by the U.S. Department of Health and Human Services' Office for Civil Rights and the Occupational Safety and Health Administration in the current regulatory environment for comparable facilities; what analytical procedure HIPAA provides for determining whether a security incident is subject to mandatory reporting; and what the regulatory context of the state of Florida is, which supplements federal standards. The internal focus of the work was on mapping the identified risk areas to existing operational checklists and designing compliance audits as an additional layer on top of them.

ISSN: 2787-9364

Results

The integrated system developed in this study is hereinafter referred to as the Integrated Compliance Operations Framework (ICOF). The framework consists of five interconnected components - a compliance risk classification system, a four-factor procedure for assessing potential violations, a three-tiered photographic authorization system, a daily compliance checklist, and a staff training model - unified by a single organizing principle: regulatory requirements are embedded into the facility's existing operational rhythm rather than maintained as a separate audit cycle.

1. Compliance Risk Classification System

The first step was to sort the identified gaps by practical urgency. Each gap was assessed along two dimensions: the likelihood of occurrence under the facility's existing operational routines, and the severity of potential legal or reputational consequences if left unresolved. Prioritization was necessary - the system had to identify what required immediate attention rather than produce an undifferentiated list of weaknesses. Gaps where both dimensions were simultaneously significant were addressed first; the remaining items formed a documented remediation schedule to be resolved progressively.

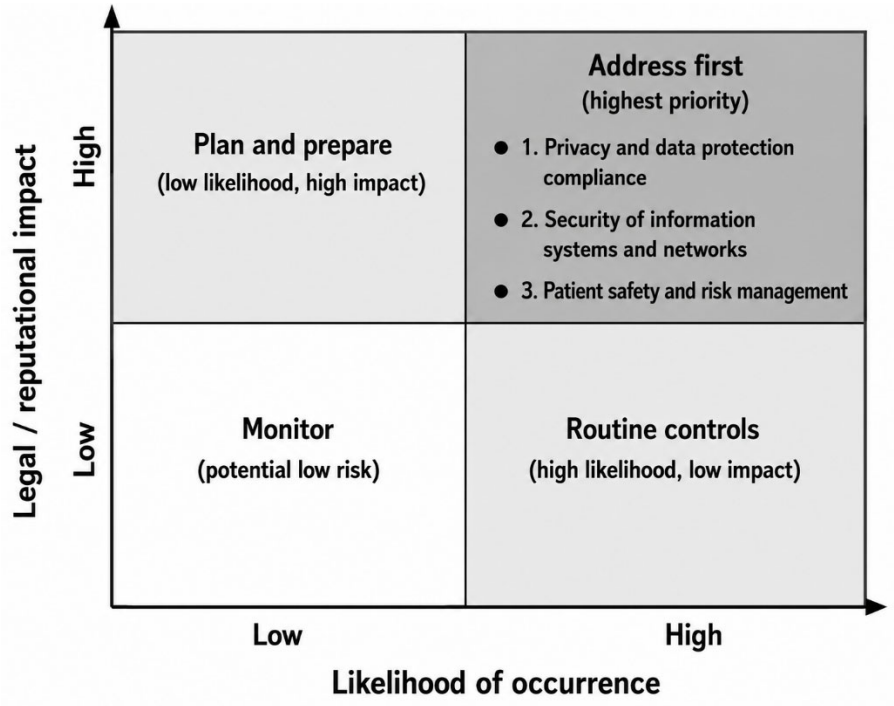

Figure 1. Compliance risk classification system based on likelihood and legal/reputational impact

The external expert confirmed that the three highest-priority risk categories identified are consistent with current national enforcement priorities of the U.S. Department of Health and Human Services' Office for Civil Rights and OSHA - and are not unique to the study site but represent the most common compliance gaps across small outpatient aesthetic facilities. These categories are: patient photographic documentation authorization, where the absence of clear distinctions between clinical, marketing, and educational use creates ambiguity; the security of medical information transmission channels, where informal practices develop in the absence of defined procedures; and biohazardous materials management, where training protocols and exposure logs - including sharps injury and exposure incident records - require formal integration into daily operational workflows.

2. Four-factor procedure for assessing potential violations

Among the insights that the external expert contributed to the system's development - and which could not be obtained through independent study of publicly available regulatory texts - the analytical procedure prescribed by HIPAA to determine whether a detected security incident is subject to mandatory reporting to the regulator and affected patients was of particular practical value.

ISSN: 2787-9364

The procedure covers four factors: the nature and scope of the medical information involved and the likelihood of identifying a specific patient; the person who gained unauthorized access to the information or used it; the extent to which the information was actually disclosed to third parties; and the extent to which the risk was mitigated after the incident was detected [13].

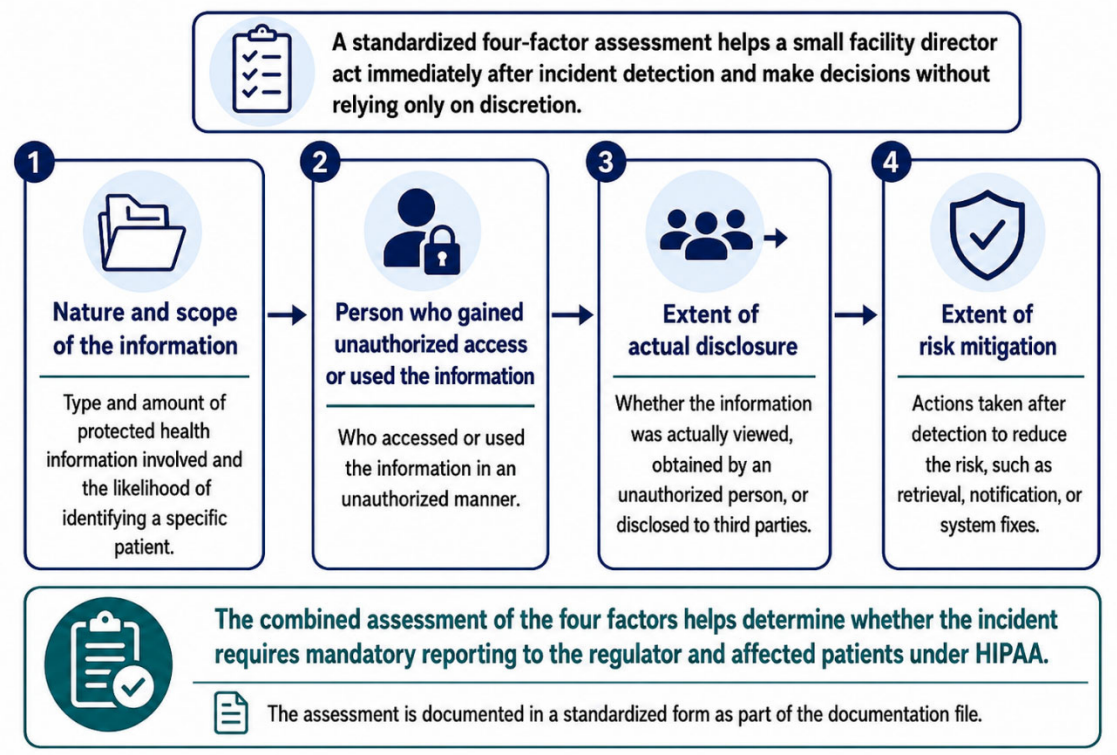

Figure 2. Four-factor procedure for assessing potential compliance violations

The director of a small facility facing a potential security incident typically faces a practical dilemma: either immediately engage an outside attorney or act at their own discretion. A four-factor procedure, documented in a standardized form as part of the documentation file, resolves this dilemma: an assessment based on these four factors can be performed immediately upon detection of the incident, and decisions regarding further actions can be made based on its results.

3. Three-Tiered Authorization System for Photographic Documentation

Photographing patients before and after aesthetic procedures serves several distinct functions within the clinic's operations: clinical documentation of results and safety, marketing use in external materials, and staff training and education. Each function has a separate legal framework under HIPAA, and combining all three into a single informed consent document creates ambiguity, which is a direct source of compliance risk.

The first document covers photography for clinical documentation and monitoring of treatment outcomes. It is mandatory at the first visit and at the start of each new course of treatment, and photographs taken under it are stored exclusively in the medical information system and may not be used outside the clinical setting.

The second document covers permission for marketing use of photographic materials. It is voluntary, specifies permitted usage formats and the degree of patient identifiability, and preserves the patient's right to revoke consent at any time without consequences for care - voluntariness and revocability being HIPAA requirements for valid authorization.

The third document covers the use of a patient's clinical results in educational or scientific materials, kept separate from marketing consent so staff can use clinical records for training without obtaining renewed consent each time.

ISSN: 2787-9364

The three-tier system resolved an operational issue that preceded the legal one: staff received clear answers to the question "which photo to store where and for what purposes," whereas prior to the system's implementation no standardized guidance existed for these decisions across the facility.

4. Daily Compliance Checklist

The daily compliance checklist was not created as a separate system with its own schedule and designated personnel. Regulatory checks are built directly into the checklist that staff use daily to monitor office occupancy, material inventory, and adherence to patient care protocols.

Daily checks cover issues that arise during each shift: whether patient records in the medical information system are closed at the end of the day; whether medical information was sent via staff members' personal devices; whether sharps containers have been checked; and whether all new patients have signed authorization forms prior to their first procedure. The weekly level adds a check of the security of online appointment booking channels [4], confirmation that photos from the current week have been transferred to the medical information system and deleted from personal devices, and verification of the validity of agreements with software vendors.

The monthly level involves reviewing the complete list of technology service providers with access to patient medical information and verifying the existence of agreements with each of them; reviewing the register of potential security incidents and applying a four-factor procedure to each identified case; and providing documented confirmation that the annual occupational safety training cycle is on schedule.

5. Staff Training Methodology

Compliance training is integrated into the same four-week new employee orientation program, during which new hires simultaneously learn clinical protocols, operational standards, and patient care guidelines. HIPAA and OSHA topics are not covered in a separate legal course - they are introduced in the context of specific operational scenarios.

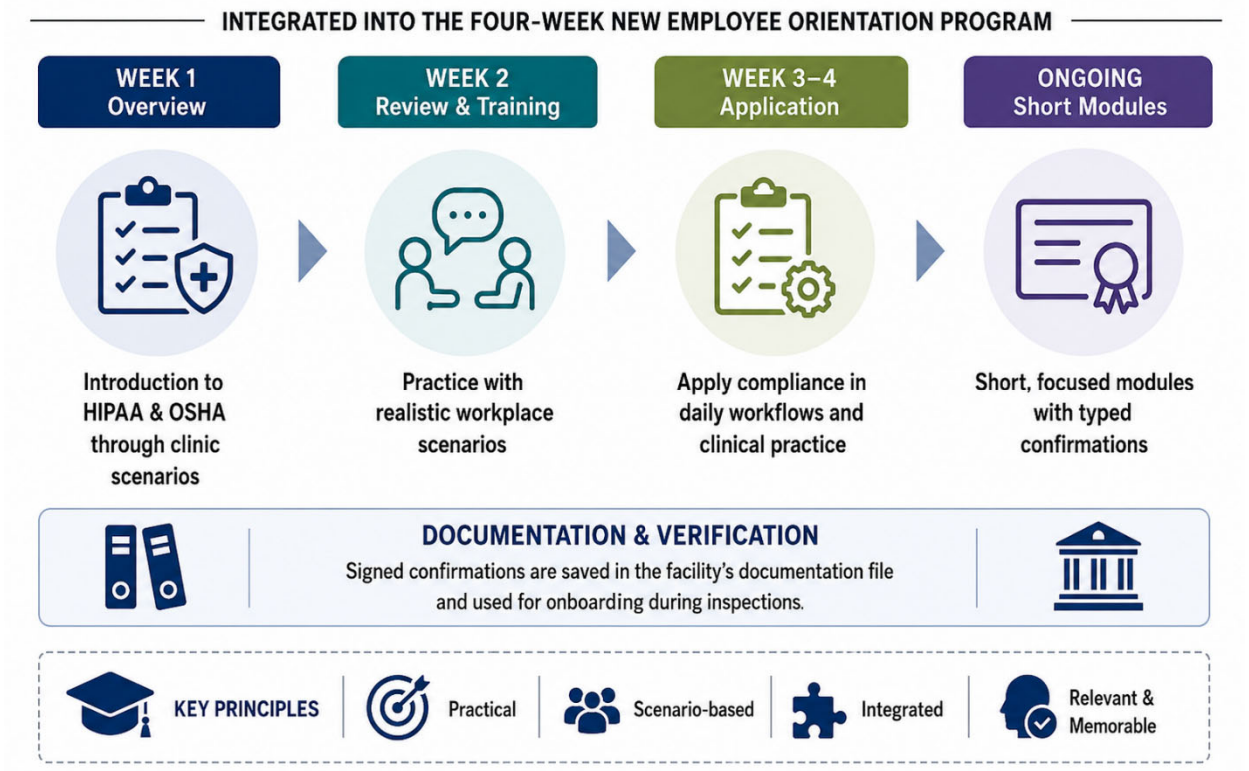

Figure 3. Staff training methodology integrated into the four-week new employee orientation program

During the first week, new employees receive an overview of HIPAA and OSHA requirements in a format focused on specific scenarios from the clinic's practice, rather than a recitation of regulatory text. Instead of stating, "It is prohibited to transmit protected health information via

ISSN: 2787-9364

unsecured channels," the training explains that sending a patient's photo to a group chat constitutes a violation even when all chat participants are clinic employees.

During the second week, the training shifts to realistic workplace scenarios. Employees practice how to respond when a patient asks for their photos to be sent to a personal email, when someone requests the publication of before-and-after images on social media, when a colleague asks about another patient's procedure, or when an unrecorded needle stick incident is discovered. These exercises are built around situations staff may actually encounter, so the focus is on practical response rather than formal knowledge testing. As a result, the training feels less intimidating and the procedures are easier to retain.

Annual recertification training in accordance with OSHA standards is conducted in several short thematic modules. All sessions are documented with signed confirmations, which are stored in the facility's documentation file and serve as the basis for verification during scheduled or unscheduled inspections.

6. External Consultation Model

An external specialist was engaged in two modes. The initial consultation addressed three questions that could not be answered through independent study of regulatory texts: current enforcement priorities of the U.S. Department of Health and Human Services' Office for Civil Rights and OSHA, the HIPAA analytical procedure for assessing a potential violation, and Florida-specific regulatory requirements that supplement federal standards. The expert also assessed what level of documentation completeness meets HIPAA administrative safeguards requirements for a facility of this size and complexity.

Following the initial system design, the consultation shifted to an annual maintenance mode of one to two hours per year, focused on regulatory changes over the past year, continued fit with the network's current scale, and priorities for the coming year in light of enforcement trends. This model keeps regulatory knowledge current and provides independent verification of the system without the cost of a full-scale audit.

7. Audit and Resolution of Business Associate Agreement Coverage

One outcome of the initial consultation with the external compliance specialist was a structured review of Business Associate Agreement coverage across all technology vendors with access to patient medical information. Under HIPAA, a covered entity bears regulatory responsibility for the data handling practices of its business associates regardless of where a breach originates [7], making a complete and current inventory of such agreements a foundational element of any integrated compliance system.

The review found that the existing agreement inventory did not yet cover the full range of vendors operating within the facility's technology environment. Several patient-facing and communication platforms with access to protected health information were identified as requiring assessment and, where applicable, formal agreement documentation.

Addressing this gap was straightforward once the inventory was complete. Agreements were reviewed and formalized with all relevant vendors. Ongoing verification of Business Associate Agreement coverage for all current and new technology vendors has since been incorporated into the monthly compliance checklist, ensuring that future vendor additions are assessed before access to patient information is granted rather than identified retrospectively.

8. System Rollout

Following implementation at the main facility in Miami, the system was replicated at the Tampa and Ocala locations; implementation was ongoing at Coconut Creek at the time of writing. Six external facilities - four independent clinics and two cosmetic studios, which expand the scope of services to include medical aesthetic procedures - implemented individual elements of the system independently. This replication was made possible because the system is documented in the form of specific operational materials: standardized three-tier authorization forms, daily checklist templates, scenarios for practical simulation exercises for training, and a four-factor assessment form for potential violations. All materials are designed for use by a director without specialized legal training.

ISSN: 2787-9364

9. Quantitative Outcomes

Across the full study period - March 2024 through February 2026 - the facility recorded no HIPAA breaches, no OSHA citations, no regulatory investigations, and no patient complaints related to privacy or data handling. No sharps injuries were documented over the same period, reflecting the effectiveness of the disposal protocols embedded in the room setup and turnover checklists. One photographic-authorization near-miss was identified through the social media content review process and resolved before any publication occurred, preventing an unauthorized disclosure of protected health information. Business associate agreements were concluded with all relevant vendors. The facility also passed a formal external inspection conducted by an environmental health officer with no corrective actions required, providing independent third-party validation across sharps safety, chemical management, sanitation, laser safety, and staff training documentation. Because compliance checks were embedded into workflows that staff already performed, the integration added no dedicated compliance hours; for a team of roughly ten to fifteen people, this displaced an estimated one hundred to two hundred twenty-five staff hours per month that the parallel-system model devotes to managing compliance separately. No compliance-related disciplinary actions or terminations occurred during the period, suggesting genuine behavioral adoption rather than surface compliance.

DISCUSSION

1. Compliance and Operational Efficiency: A False Dichotomy

The central contribution of this work is methodological rather than regulatory: the requirements are well known, but their integration into the operational fabric of a small facility is what distinguishes the proposed framework from the conventional annual-audit model.

The common management paradigm that views regulatory compliance and operational efficiency as inversely related contradicts the practical experience described in this article. In each of the implemented system components, HIPAA and OSHA requirements either address the same operational problem that was already a focus for management, or are a direct consequence of decisions already made in the operational context.

The most illustrative example in this regard is the three-tiered photo authorization system. Prior to its implementation, staff encountered recurring uncertainty about: whether a specific photo could be shared with the marketing department; whether a patient needed to sign additional documents; or how to handle a request via social media. This uncertainty caused operational disruptions regardless of the legal risk. Three separate authorization forms resolved both the operational and legal issues together, which is why the implementation was accepted much more readily than if it had been justified solely by legal arguments.

A similar dynamic is evident in the integration of regulatory checks into the daily checklist. The requirement to verify that open patient records are closed at the end of the shift aligns with the operational requirement to complete documentation by the next day. The requirement to verify that photographs have been uploaded to the medical information system aligns with the requirement for proper clinical documentation of results. A compliance check and an operational standard turn out to be descriptions of the same action from different perspectives.

2. Changes in Staff Behavior

Staff resistance to the implementation of compliance checks turned out to be significantly lower than in the case of implementing performance measurement systems. The difference in reaction stems from how staff perceive the nature of the new requirements. Performance requirements affect self-esteem and are taken personally. Compliance requirements, presented as protection for patients and the staff themselves from legal consequences, align with how healthcare staff understand the purpose of their work.

Once staff understood the specific mechanisms by which familiar informal practices - such as sharing clinical images through undesignated communication channels - constitute compliance risks, behavior changed without any additional enforcement measures. This result confirms Nilsen's thesis

ISSN: 2787-9364

that the long-term adoption of new practices requires an understanding of their logic, not merely the fact of their existence. [10]

3. Annual Consultation for Institutions with Limited Resources

The experience of engaging an external specialist points to a practical conclusion about the optimal model for small institutions: what mattered most was not the number of consultation hours but the quality of the questions asked. The three questions addressed in the initial consultation (Section 4.6) supplied exactly what independent study of regulatory texts could not, since publicly available HIPAA and OSHA materials describe requirements without prioritizing them or reflecting current enforcement practice.

The annual maintenance format - a single one- to two-hour session - keeps the system current without the expense of a full audit, offering a replicable model for small-facility directors with limited budgets for legal support.

4. Limitations of the Study

The system was developed and tested under operational conditions in the state of Florida, which has a specific regulatory context. Implementation in institutions in other states requires prior verification regarding regional regulations. This article describes management experience and is not a source of legal advice; for each specific facility, engaging a qualified professional for initial verification of the system is mandatory.

CONCLUSIONS

The experience of Arviv Medical Aesthetics points to a broader conclusion: compliance works best when it is built into everyday operations. Instead of relying mainly on an annual audit, the ICOF made regulatory checks part of routine workflows. This helped the facility maintain more consistent compliance without increasing the administrative burden on staff.

Among the operational lessons learned during implementation, several are recurring regardless of the facility's size. Authorization of photographic documentation, protection of medical information transmission channels, and management of biohazardous materials remain the most vulnerable areas in the current regulatory environment. Three-tiered photo authorization was implemented with less resistance than other changes - because it addressed a specific operational hassle that staff experienced daily, rather than just an abstract legal risk. Verifying the existence of agreements with software vendors that have access to patients' medical information should be prioritized: it takes only a few hours, is a one-time fix, and addresses a category that consistently ranks among the priorities of ongoing investigations by federal regulatory agencies.

Engaging an external specialist on an annual basis - targeted at three specific issues - proved to be a more effective model than a comprehensive audit, in terms of the ratio of knowledge gained to resources expended. This model can be recommended to institutions with limited budgets for legal support as a replicable and practically realistic approach.

The framework has demonstrated reproducibility and scalability: it was replicated across four network locations and adopted, in whole or in part, by six independent external facilities without the involvement of the original author. Because every component is documented as concrete operational materials - standardized authorization forms, checklist templates, training scenarios, and an assessment form - the system can be transferred to other clinics and operated by a director without specialized legal training. This makes the framework of direct practical use to the broader outpatient aesthetic sector, where most facilities lack a dedicated compliance department.

Prospects for further research include the development of a standardized tool for assessing the maturity of compliance management in small and medium-sized aesthetic clinics, as well as investigating whether the level of such maturity affects clinical safety and patient satisfaction - a question that remains open.

ISSN: 2787-9364

3REFERENCES

1. American Med Spa Association (AmSpa). (2023). 2023 State of the Medical Spa Industry Report. American Med Spa Association. https://www.americanmedspa.org/page/industry-stats

2. Grand View Research. (2024). Medical Spa Market Size, Share & Trends Analysis Report. Grand View Research, Inc. https://www.grandviewresearch.com/industry-analysis/medical-spa-market

3. Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act drove large gains in hospital electronic health record adoption. Health Affairs, 36(8), 1416–1422. https://doi.org/10.1377/hlthaff.2016.1651

4. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

5. IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation. https://www.ibm.com/reports/data-breach

6. Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Communications Inc. https://www.verizon.com/business/resources/reports/dbir/

7. U.S. Department of Health and Human Services, Office for Civil Rights (HHS OCR). (2023). HIPAA Enforcement Highlights. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-highlights/index.html

8. Occupational Safety and Health Administration (OSHA). (2023). Bloodborne Pathogens Standard (29 CFR § 1910.1030). U.S. Department of Labor. https://www.osha.gov/bloodborne-pathogens

9. Braithwaite, J., Churruca, K., Long, J. C., Ellis, L. A., & Herkes, J. (2018). When complexity science meets implementation science: A theoretical and empirical analysis of systems change. BMC Medicine, 16(1), 1–14. https://doi.org/10.1186/s12916-018-1057-z

10. Nilsen, P. (2015). Making sense of implementation theories, models, and frameworks. Implementation Science, 10(1), 53. https://doi.org/10.1186/s13012-015-0242-0

11. Brandão, A., & Ribeiro, L. (2023). The impact of patient experience on loyalty in the context of medical-aesthetic health services. Journal of Patient Experience, 10. https://doi.org/10.1177/23743735231160422

12. U.S. Department of Health and Human Services. (2023). HIPAA for Professionals: Privacy. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

13. Office of the National Coordinator for Health Information Technology (ONC). (2023). Security Risk Assessment Tool. HealthIT.gov. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

ISSN: 2787-9364