SMILE & BREW DENTAL CLINIC

A CASE STUDY ON THE APPLICATION OF INFORMATION ASSURANCE, SECURITY AWARENESS, AND TRAINING

Aliman, Jachin Adam E. | Bugayong, Klein William S. | Lalata, Christine Joy D. | Lim, Frances Aura D. | Paragas, Jerwin Claus J.

PHINMA University of Pangasinan

ITE 302: Information Assurance and Security

Mr. Kris C. Calpotura, DIT

September 2025

TABLE OF CONTENTS

1. INTRODUCTION

1.1 About the Organization

Smile & Brew Dental Clinic is a private dental institution operating as a Sole Proprietorship. Despite its small size, with a team of one chief dentist, three associate dentists, and six dental assistants, the clinic is committed to its mission of "To deliver quality dental care with compassion, comfort, and a smile" and a vision "To be the trusted clinic that creates healthy smiles in a warm, welcoming space". It serves individuals of all ages, providing a range of services from routine check-ups and cleanings to cosmetic dentistry. While its core operations have traditionally been paper-based, the clinic has embraced technology for social media advertising and booking, and digital record-keeping, specifically for panoramic x-rays.

However, this reliance on technology and the handling of sensitive patient information have introduced new security challenges. Issues such as the lack of backups for physical records, lack of personnel for physical security, minimal cybersecurity tools, and a reliance on an external IT technician who is only hired when a problem arises, have become evident. The clinic recognizes these realities, and acknowledges that a data breach could lead to a loss of patient trust, legal consequences, and financial loss. Thus, information security is a crucial consideration for the clinic as it strives to protect sensitive data and maintain its reputation in the community.

1.2 Why Choose This Organization

Smile & Brew Dental Clinic was chosen as a case study because it represents a critical and often-overlooked segment in information security: a small business with limited resources that handles highly sensitive data. Unlike large healthcare organizations, this sole proprietorship operates with a small team and a minimal IT infrastructure. The clinic's unique blend of traditional paper-based record-keeping and modern digital processes creates a distinct set of vulnerabilities.

The case study provides valuable insights into the challenges faced by such under-resourced organizations, which must balance the need to use technology with the realities of limited funds and a small staff. For example, the clinic's lack of digital backups for its physical patient records exposes it to the risk of permanent data loss in the event of a disaster, such as a fire or flood. The reliance on a single, on-demand external IT technician also highlights the risk of delayed response to technical security incidents. Examining these challenges can serve as a model for other small businesses experiencing similar conditions, demonstrating how even modest, practical security measures, such as implementing proper data backup procedures and enhancing staff security training, can significantly improve resilience and protect both patient data and the business's reputation.

1.3 About the Team Members

The success of this project relied on the collaborative efforts of a five-member team, each contributing distinct expertise that ensured a thorough and balanced study of Smile & Brew: Dental Clinic. The specialization of roles allowed the team to approach the research systematically—beginning with accurate data collection, followed by threat and risk assessment, and culminating in the development of practical recommendations to strengthen the clinic's information security and operational resilience.

Each member of the team undertook a distinct role, ensuring that the research process was systematic, comprehensive, and aligned with the project's objectives:

Project Lead & Information Gathering Specialist – As a Project Lead & Information Gathering Specialist, Ms. Lim was responsible for the strategic direction of the research initiative. She defined the study's objectives, designed a framework tailored to Smile & Brew Dental Clinic, and guided the team through each phase of the process. This role also required her to be the primary point of communication with the client organization, engaging directly with clinic personnel to collect necessary information for this case study. She was also responsible for coordinating tasks among team members, ensuring research standards were met, and maintaining alignment with the clinic's mission and vision, ultimately synthesizing the team's analyses into a comprehensive and well-structured final report.

Scope Analyst – Ms. Lalata was instrumental in shaping the initial phase of the case study. As Scope Analyst, she was responsible for defining the project's purpose and ensuring its objectives aligned with the data available from Smile & Brew Dental Clinic. This role required her to meticulously analyze the provided information to determine what was feasible for the study and to outline the project's scope. Ms. Lalata also took charge of documenting the team's composition, ensuring a clear record of each member's role and contribution from the outset of the project.

Threat & Risk Assessment Specialists – Serving as the evaluators of Smile & Brew Dental Clinic's security posture, Mr. Paragas & Mr. Bugayong was responsible for identifying potential threats and assessing risks associated with both physical and digital operations. This role involved examining vulnerabilities in record-keeping, cybersecurity practices, and reliance on external IT support, while also considering the clinic's limited resources and operational realities. Mr.

Paragas & Mr. Bugayong analyzed the likelihood and impact of these risks, ensuring that the findings guided the development of practical and effective recommendations for safeguarding sensitive patient information.

Security Controls Researcher – Serving as the strategist of the research initiative, Mr. Aliman was responsible for formulating actionable solutions based on the team's findings on Smile & Brew Dental Clinic. This role involved translating identified risks and vulnerabilities into practical recommendations that aligned with the clinic's mission, vision, and operational capacity. Mr. Aliman ensured that the proposed measures were realistic, sustainable, and capable of strengthening the clinic's information security while supporting its goal of delivering quality dental care.

1.4 Recommended Organizational Members

Based on the document, it's clear there is no one dedicated to security, as the clinic owner coordinates all security responses, while an external technician handles technical fixes. For a small organization like Smile & Brew, a full-time security team isn't practical. Instead, here are suggested members or roles and their contributions to strengthen the clinic's security posture:

1. **Designated Security Officer**

This role would be assigned to an existing staff member, like the clinic owner or a senior assistant. The goal isn't to make them an IT expert, but to give them a clear, documented responsibility for security oversight.

Policy Development and Enforcement: They would be responsible for creating and enforcing formal, written security policies. This includes detailed rules for handling patient information, creating strong passwords, and a clear incident response plan for events like a lost device or a virus infection.

Security Training: They would manage a schedule for regular security training for all staff, going beyond the initial onboarding to include specific topics like how to spot fake emails and other scams.

Coordination: They would be the central point of contact for all security-related matters. Instead of the owner, this person would coordinate with the external IT technician and other vendors to ensure security issues are addressed in a timely manner.

2. **External Security Consultant (vCISO)**

A virtual Chief Information Security Officer (vCISO) is an external professional who provides expert guidance on an as-needed basis. This role fills the gap in strategic security planning without the cost of a full-time employee.

Risk and Vulnerability Assessments: They would conduct a formal risk assessment to identify vulnerabilities beyond what the clinic has already recognized.

Strategic Planning: They would help develop a long-term security strategy that aligns with the clinic's business goals, ensuring security practices are not just reactive but proactive.

Vendor Management: They would draft security-related clauses for contracts with third-party vendors, such as external IT providers or insurance companies, ensuring they adhere to professional security standards.

3. **Security Personnel / Security Guard**

This role focuses on the physical protection of the clinic’s premises, staff, patients, and sensitive assets. While the clinic already uses CCTV and locked entrances, assigning or contracting a security guard provides an added layer of assurance.

Premises Protection: The guard would monitor entry points during operating hours and ensure that only authorized individuals have access to treatment and record-storage areas.

Incident Response: In the event of theft, intrusion, or unauthorized access attempts, the guard would act immediately to contain the situation, report it to management, and coordinate with authorities if needed.

Patient and Staff Safety: Beyond protecting property, the guard’s presence would also provide reassurance to patients and employees, ensuring a safe and welcoming clinic environment.

2. PURPOSE OF THE PROJECT

The primary purpose of this study is to explore and evaluate the implementation of information security procedures, awareness, and training within the context of a small healthcare facility—Smile & Brew Dental Clinic. Regardless of their size, Smile & Brew Dental Clinic is responsible for collecting, handling, storing, and protecting highly sensitive personal and medical information, the importance of robust information security practices cannot be overstated. In an era where data breaches and cyber threats are increasingly common, even small clinics are becoming vulnerable targets due to limited technological infrastructure, lack of dedicated IT personnel, and minimal formalized security protocols.

This study specifically seeks to examine the extent to which Smile & Brew Dental Clinic understands and applies information security awareness and training among its staff and how this affects the clinic's overall ability to protect patient data. It aims to investigate the clinic's current practices in securing both physical and digital patient records, the level of awareness and engagement of employees regarding information security threats (such as phishing, data leakage, and unauthorized access), and the adequacy of the policies and procedures currently in place to ensure data confidentiality, integrity, and availability.

Additionally, the study intends to assess the alignment of the clinic's practices with existing legal and ethical standards, particularly the Data Privacy Act of 2012 (Republic Act 10173) and relevant Department of Health (DOH) guidelines on health data protection. It will also evaluate the technical, administrative, and physical safeguards being used within the clinic and how these are supported by employee training and awareness initiatives.

Through qualitative data gathering, including observation, documentation analysis, and interviews, the research aims to identify gaps in current practices and highlight areas where the clinic is performing well. It will also explore the challenges faced by small healthcare providers in implementing information security policies effectively—such as lack of financial resources, minimal IT support, and reliance on paper-based systems.

Lastly, this study seeks to provide recommendations that can help Smile & Brew: Dental Clinic strengthen their information security framework through improved training, enhanced policy development, and better integration of affordable technologies. By doing so, the study contributes to the broader discourse on how even micro and small enterprises in the healthcare sector can implement feasible, scalable, and effective information security practices to safeguard the privacy and trust of their patients.

3. IDENTIFIED RISKS

3.1 Threat Identification

It is unavoidable to have the presence of threats in every organization. Smile & Brew Dental Clinic is not an exception to this. Threats may be as small as a phishing to disasters that compromise everything an organization has worked hard for. In order to keep operations and business objectives under control, anticipation of these threats is the first step to do. Listed below are categories of threats and possible issues that the dental clinic may encounter:

Inadvertent Acts. Due to verbal implementation of security policies, there's a chance that employees may forget the rules and unintentionally perform activities that put critical information at risk. For example, an employee might inadvertently share a patient's personal information during a casual conversation if they aren't explicitly reminded about data privacy protocols. Furthermore, without a formal, written policy, an employee who manages the clinic's social media pages might click a malicious link or fall victim to a scam that compromises their personal device. Even though they don't have the main account's login credentials, this could lead to the scammer gaining control of the clinic's social media and posting damaging content, causing reputational harm and a loss of patient trust.

Deliberate Acts. As pointed out, the lack of a formally-implemented document for security policies increases the risk of deliberate acts by both external and internal threats. Because the clinic's patient data is primarily physical, an internal threat, such as a disgruntled employee, could intentionally steal or destroy records. The absence of a clear, written chain of custody for these physical records makes it difficult to track who has accessed them. A current employee with authorized access could deliberately post malicious content or leak sensitive information to cause harm. Without a clear, written policy on what can or cannot be posted on the clinic's social media pages, it is difficult to hold an employee accountable for these deliberate actions. As for external deliberate acts, the installation of a tinted sliding door may not be enough when an armed person comes into play.

Environmental Threats. Especially in the Philippines, it is unavoidable for organizations to encounter natural disasters like typhoons, earthquakes, and fires. By the time these environmental disasters strike, the physical records, digital devices, and machineries that Smile & Brew owns may be put at risk. Upon being exposed to these threats and receiving damage, especially for physically-kept patient records, it might need a stretch for the dental clinic to recover. Without a formal backup and recovery plan that includes off-site data storage and a comprehensive strategy for restoring operations, the clinic would face significant challenges in recovering from such an event.

Technical Failure. With the regular clinical dentistry process requiring the use of electricity-powered machines, it is important that operations are kept powered. Especially with how unpredictable power outages can be in the Philippines, there is a possibility that ongoing dental procedures may be put at a halt if there are no backup power sources available, and it might compromise a patient’s wellbeing. Aside from that, a technical failure could also result from malware or a virus that corrupts the clinic's digital patient records, rendering them unreadable and unusable, if the clinic does adapt to digital information storage means.

Management Failure. The organizational structure of Smile & Brew consists of 1 chief dentist, 3 associate dentists, 6 dental assistants. Currently there being no dedicated personnel in charge of security, all responsibilities for keeping operations running smoothly and securely are taken care of by the chief dentist. The absence of a dedicated IT or security professional means that the chief dentist, in addition to their primary medical responsibilities, must take on the crucial, time-consuming, and often technical role of managing all security matters. This can create a significant burden and lead to potential oversight. The reliance on external IT technicians who are only hired for specific, reactive problems also means there is no one proactively monitoring for threats, conducting regular security audits, or implementing new security measures to prevent issues before they occur. This reactive approach to security leaves the clinic vulnerable to threats that could have been prevented with consistent, in-house management.

3.2 Vulnerability Identification

Here is a list of identified vulnerabilities that correspond with the threats that have been identified:

1. Lack of Formal IT Security: No dedicated firewall, intrusion detection, or proactive monitoring.
2. No Digital Data Backup: Digital panoramic x-rays are stored on a single desktop's local storage with no backup system. A single hardware failure or ransomware attack would result in permanent data loss.
3. Inadequate Physical Security for Data: Highly sensitive physical records are stored in a single cabinet. There is no off-site backup (e.g., digitized copies) or fireproof/waterproof safe, making them vulnerable to a single disaster.
4. Lack of Formal Access Control Procedures: While access is restricted to staff, there is no detailed log of who accessed which record and when. Revoking access for former employees relies solely on them returning keys, with no digital audit trail.
5. Single Points of Failure: One desktop holds all digital data; one cabinet holds all physical data.
6. No Documented Incident Response Plan: No clear steps to follow in case of a breach or disaster.

7. Basic Wi-Fi Protection: Network is secured only with a password, lacking advanced encryption segmentation.
8. Reactive IT Support: No strategic security guidance, only break-fix support.

3.3 Risk Assessment

The next key part is to assess the risks involved with the threat, with its likelihood and its severity or level of impact. The following are the threats stated before with the inclusion of its risk severity and likelihood.

Fire/Flood destroying physical patient records and the digital desktop (No backups). This is the worst-case scenario. The complete loss of all patient data would halt operations, cause immense reputational damage, and lead to significant legal penalties under the Data Privacy Act. The impact is catastrophic (Severity: 5). While the likelihood of a major fire is low (1) , the vulnerability of the data is extreme, making the overall risk very high.

Ransomware infection on primary desktop (No backups, critical data stored there). Ransomware attacks are increasingly common and target healthcare providers. The impact would be high, as the clinic would lose access to all digital x-rays and could be extorted for money. The likelihood is medium due to the lack of advanced protections (Severity: 5, Likelihood: 3). Overall risk: Very High.

Theft or unauthorized access of physical patient records (Single cabinet, no detailed access logs). The impact of a physical data breach is very high, leading to loss of patient trust and legal action. The likelihood is medium; while the clinic is physically secure during the day, the cabinet itself is a vulnerable target (Severity: 5, Likelihood: 2). Overall risk: Very High.

Data breach via hacked social media/booking platform (External facing, mentioned concern). A breach here could lead to defacement, stolen patient data from the booking system, or fraud. The impact is high for reputation. The likelihood is medium, as these platforms are common attack vectors (Severity: 4, Likelihood: 3). Overall risk: High.

Former employee accessing patient data (No formal access revocation process). This is a high-impact breach of confidentiality (Severity: 5). The likelihood is low to medium (2), dependent on the intent of the former employee, but the vulnerability makes it possible. Overall risk: Very High.

Loss of digital x-ray data due to hardware failure (No backups). Hard drive failure is a common technical occurrence. The impact is high, as those patient records are permanently lost (Severity: 4, Likelihood: 3). Overall risk: High.

3.4 Risk Management

The next step is to manage the risks involved in the clinic. This is done after risk assessment and the process results in either mitigating or reducing the risk, transferring the risk (e.g., through insurance), eliminating the risk entirely, or accepting the risk if it is within the organization’s risk appetite.

For the high-risk scenarios involving data loss (fire, ransomware, hardware failure), the primary strategy is mitigation through technical and physical controls. The risk can be almost entirely eliminated by implementing a 3-2-1 backup rule (3 copies, on 2 different media, 1 copy off-site). This involves immediately starting to back up digital x-ray files to both an external hard drive and a secure, encrypted cloud service. Furthermore, the risk is reduced by creating digital copies of physical records and including them in this new backup regime, ensuring a disaster doesn't destroy the only copy.

For risks involving unauthorized access (theft, former employees), the strategy is mitigation through administrative and physical controls. This involves formalizing access control with a sign-in/sign-out log for the physical cabinet and a strict offboarding checklist for key return. To mitigate digital access risks, the clinic must enhance basic cybersecurity by ensuring strong Wi-Fi encryption (WPA2/WPA3) and installing reputable, updated antivirus software on all machines.

For the risk of a breached external system (social media/booking), the strategy is mitigation through administrative controls. This requires implementing ongoing security training for all staff, with a specific focus on phishing awareness to teach them how to identify fraudulent emails attempting to steal login credentials for these platforms.

For the overarching risk of poor preparedness (management failure), the strategy is mitigation through administrative controls. The clinic must develop an Incident Response Plan—a simple document outlining steps to take during a breach—and review physical security measures, such as considering a fireproof safe for the most critical records. The long-term goal to eliminate multiple vulnerabilities is to adopt a Clinic Management Software solution that provides built-in security, encrypted backups, and proper access logs. For risks that cannot be fully mitigated, such as the financial impact of a major fire, the strategy should include transferring the risk through comprehensive business insurance.

4. RECOMMENDATIONS

4.1 Security Recommendations

For Accidental Data Loss. Accidental deletion or misplacement of patient records, appointment schedules, or financial documents poses a major threat to the clinic's operations. To address this, Smile & Brew Dental Clinic should implement regular information security awareness training for all staff, emphasizing proper handling and storage of files. Automated cloud backup systems such as Google Drive or Microsoft OneDrive should be adopted to ensure that all digital records are continuously synchronized and recoverable. Additionally, version history and recovery options must be enabled to allow quick restoration of files in case of unintentional deletion.

For Deliberate Physical Acts. Physical threats such as theft or tampering with clinic computers and dental equipment can disrupt operations. To reduce this risk, the clinic should install CCTV cameras at entry points, server rooms, and storage areas, with recordings secured and reviewed regularly. Security locks should be used on computers containing sensitive data, and server or networking equipment should be placed in access-controlled rooms. The clinic should also enforce strict visitor access protocols, ensuring only authorized personnel can enter restricted areas.

For Deliberate Cyber Attacks. As the clinic stores sensitive patient records, cyber threats such as phishing, ransomware, or brute force attacks are a significant risk. The clinic should adopt a properly configured firewall and Intrusion Detection System (IDS) to monitor unusual traffic patterns. Regular system updates and antivirus scans must be enforced on all computers. Staff should undergo cybersecurity training to identify phishing emails and suspicious links. Multi-Factor Authentication (MFA) should be implemented on systems containing patient or financial data to reduce the risk of unauthorized access.

For Natural Disasters. Hazards such as floods, earthquakes, or fires can damage both physical records and IT systems. To mitigate this, essential servers and critical records should be stored in waterproof and fireproof cabinets. Digital copies of important patient data and financial files should be backed up to secure off-site cloud servers, ensuring business continuity in case the physical clinic is compromised. A documented disaster response plan must be created, outlining procedures for evacuation, asset protection, and data recovery.

For Technical Failures. Power interruptions, internet outages, or hardware malfunctions can disrupt the clinic's services. To minimize these risks, all critical devices, especially servers and dental management systems, should be connected to Uninterruptible Power Supply (UPS) units. Surge protectors should be installed to safeguard against electrical spikes, and a backup generator should be procured to maintain operations during extended blackouts. For internet reliability, the clinic should maintain a secondary mobile data option to ensure that appointments, billing, and communication with patients remain functional.

For Management Failures. Insufficient IT oversight or lack of proper planning can worsen existing vulnerabilities. To address this, Smile & Brew Dental Clinic should designate or hire an IT support specialist responsible for system maintenance, cybersecurity, and data backup. If hiring is not possible, outsourcing IT services to a trusted provider is recommended. The clinic should also develop a formal IT strategy document that includes a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). These documents must be regularly updated to ensure preparedness against evolving risks.

For Lack of Organizational IT Support. Smile & Brew Dental Clinic does not have an in-house IT team and currently relies solely on external technicians who are called only when technical issues arise. This reactive setup leaves digital systems, such as the x-ray computer and online booking platform, exposed to cyberattacks, hardware failures, and potential data loss. To mitigate this risk, the clinic should consider hiring a dedicated IT staff or formalizing a continuous service agreement with a trusted IT provider. This ensures proactive monitoring, timely updates, regular backups, and rapid response to technical or security incidents, thereby strengthening the clinic's overall digital resilience.

For Lack of On-Site Security. Smile & Brew Dental Clinic relies mainly on sliding doors and tinted glass as preventive measures, but this is insufficient in case of forced entry or break-ins. To strengthen protection, the clinic should hire at least one security guard, especially during after-hours, to provide continuous monitoring and quick response to potential incidents. The presence of a guard not only deters intruders but also ensures safety for both patients and staff. This measure, combined with CCTV surveillance and strict access control to restricted areas, will significantly improve the clinic's overall physical security posture.

4.2 Security Policies

4.2.1 Recommended Authorization

For Password Policy. All clinic staff must follow strict password rules to protect sensitive systems such as patient management software and financial applications. Passwords should be at least twelve characters long, containing uppercase and lowercase letters, numbers, and special symbols. They should be updated every ninety days, and password reuse across systems must be prohibited. Sharing of passwords is strictly forbidden. Multi-Factor Authentication (MFA) should be applied to critical systems to add an extra layer of protection.

For Account Management. User accounts should follow the principle of least privilege, ensuring staff members only have the access required to perform their duties. Account access must be revoked immediately when an employee resigns or is terminated to prevent unauthorized access. Temporary account access for interns or contractors should have expiration dates and undergo regular review. Periodic audits must be conducted to verify that only authorized staff members retain access to the clinic's systems.

4.2.2 User Access Controls

For Role-Based Access Control (RBAC). Access to clinic systems and data must be based on predefined roles. For example, dental assistants may only view and update patient schedules, but they cannot access financial records. Administrative staff may process billing but should not have permission to alter patient medical histories. Only the clinic's IT administrator should have elevated privileges to maintain and configure systems, with all actions logged and monitored. This role-based structure ensures that no staff member has unnecessary access that could increase risk.

For Data Classification. Clinic data must be classified into three levels: Public, Internal, and Confidential. Public data, such as clinic operating hours and general announcements, may be shared freely. Internal data, such as staff schedules and internal communications, should be restricted to clinic personnel only. Confidential data, including patient records, medical histories, and financial reports, must be strictly protected with encryption during storage and transmission. Clear access rules must be defined, ensuring only authorized individuals can view or modify data depending on its classification.

4.3 Recommended Assessment

It is recommended that Smile & Brew Dental Clinic adopt a continuous security assessment cycle. Annually, or after any major change in operations, the clinic should re-evaluate its security posture by addressing three essential questions: What new assets require protection? What new threats or vulnerabilities have emerged? And are the current security controls still effective in addressing these risks? Regular internal audits, penetration testing, and vulnerability assessments should be conducted to ensure that policies remain relevant and effective. By maintaining this cycle of assessment and improvement, the clinic can safeguard its patient information, sustain operational continuity, and preserve its reputation as a trusted dental care provider.

5. CONCLUSIONS

This project has evaluated the information security posture of Smile & Brew Dental Clinic, a small sole proprietorship that handles highly sensitive patient data. The findings reveal that while the clinic has a strong commitment to patient care and confidentiality, its minimal IT infrastructure and reliance on traditional, paper-based systems introduce significant security vulnerabilities. The case study identified critical risks, including the lack of backups for physical and digital records, inadequate physical and technical security, and a reactive approach to IT management.

The recommendations presented in this study provide a roadmap for the clinic to strengthen its information security framework through a mix of administrative, technical, and physical safeguards. The proposed measures, such as implementing a formal data backup plan, digitizing records, and enhancing employee training, are designed to be practical and achievable for an organization with limited resources. By adopting these measures, the clinic can proactively manage risks and protect itself from potential data breaches, financial loss, and reputational damage.

5.1 Authorization

The successful implementation of the recommendations hinges on the full support and authorization of the clinic's owner and management. Formal approval is required to allocate the necessary resources and mandate the adoption of new security policies. This authorization will enable the clinic to:

- **Allocate Resources**: Secure the necessary funding and time for acquiring essential equipment, such as external hard drives, a fireproof safe, and a reliable Uninterruptible Power Supply (UPS). It also ensures that staff can dedicate time to digitizing records and participating in security training.
- **Mandate Policy Adoption**: Formally enforce security policies, such as the password policy and clean desk policy, across all staff members. This moves away from the current verbal implementation, reducing the risk of human error and deliberate acts.
- **Establish Accountability**: Formally designate an IT/Records Officer or secure a continuous service agreement with an external IT provider. This ensures there is a dedicated individual or team responsible for proactive security management, rather than a reactive, on-demand approach.

5.2 Monitoring

Continuous monitoring is crucial to ensure the long-term effectiveness of the security measures. This process will allow the clinic to adapt to new threats and vulnerabilities as they emerge. By establishing a monitoring process, the clinic can:

- **Log Review and Incident Detection**: Although data is primarily paper-based, the clinic should actively monitor logs from its online booking system and social media accounts for any suspicious activity.
- **Compliance and Policy Audits**: Periodically check that staff are adhering to new security protocols, such as using the sign-in/sign-out log for the physical records cabinet and following the formal offboarding checklist for departing employees.
- **Continuous Improvement**: Regularly assess the effectiveness of the implemented controls and make necessary updates. For example, as the clinic grows, it should reconsider its reliance on physical records and fully transition to a dedicated Clinic Management Software.

By institutionalizing a structured approach to authorization and monitoring, Smile & Brew Dental Clinic can move beyond its current vulnerabilities and build a resilient framework that protects patient data, preserves patient trust, and ensures the continuity of its operations.