# Case Study

*Design and Creative Technologies*

*Torrens University, Australia*

**Student:** Luis Guilherme de Barros Andrade Faria - A00187785

**Subject Code:** SBD 403

**Subject Name:** Secure By Design

**Assessment No.:** 2

**Title of Assessment:** Case Study

**Lecturer:** Dr. Tanvir Rahman

**Date:** Oct 2025

## Table of Contents

# Secure By Design Implementation Guide

## 1. Executive Summary

This guide defines how the organization, which happens to be an analytics company serving both hospital and retail clients, will protect critical data and maintain service continuity through Secure-by-Design (SBD) principles. The company employs roughly 300 staff divided into **100 Doctors** (hospital analytics, on premise servers) and **200 Retailers** (consumer-behavior analysis, cloud-based).

The proposed strategy integrates **people**, **process** and **technology** to meet compliance obligations under **ISO/IEC 27001, ISO 27017, NIST SP 800-53** and **OWASP Top 10 (2024)**. It balances usability and protection, embeds continuous risk management and ensures that both workgroups can operate safely without unnecessary friction.

The implementation of this strategy will follow a **phased 12-month** roadmap, ensuring that critical security controls, such as MFA, encryption and policy governance are established early, followed by staff training, continuous monitoring and final optimization. Each phase includes defined deliverables, ownership and performance metrics so that security improvements are introduced methodically without disrupting daily operations.

## 2. Context and Secure-by-Design Principles

The company processes sensitive patient and customer data across two data domains:

- **Hospital data:** stored on-prem, covered by health-privacy legislation and medical-record confidentiality.
- **Retail data:** processed in an Australian cloud environment for commercial insights.

Secure-by-Design means integrating protection at every phase of the system life cycle rather than adding controls after deployment (Shostack, 2014). The foundation rests on the CIA Triad:

- **Confidentiality**: information is available only to authorised entities.
- **Integrity**: data remains accurate and unaltered.
- **Availability**: systems and information remain accessible when required.

Complementing the CIA triad, we also have least **privilege**, **defense-in-depth**, and **human-centred security**, designing systems that people can use correctly.

## 3. User Training and Awareness Program

Human behavior remains the largest variable in cyber defense. A targeted training program to superpower human beings working for the company will include the following:

1. **Phishing awareness**: simulated phishing campaigns every quarter to reduce click-through rates and retrieve feedback on users and departments preparedness for risks.
2. **Data-classification and handling**: clear labelling of confidential, internal, and public information (ISO 27002 §8).
3. **Incident-reporting drills**: tabletop exercises teaching staff how to escalate suspicious activity.
4. **Password and MFA hygiene**: short videos showing how to use passphrases and authenticator apps.

5. **Secure remote work**: VPN use, device locking, and secure Wi-Fi guidance.
6. **HR integration**: engagement programs for performance recognition tied to cyber security certificates.

The training will be mandatory for all new hires and refreshed every six months. Progress will be tracked through the Learning-Management System and correlated with incident statistics. This aligns with **NIST SP 800-50** on security awareness and **ISO 27002 §7** on personnel controls.

## 4. Risk Assessment

Risk management follows ISO 31000 and ISO 27005, evaluating likelihood × impact – mitigation. The organisation reassesses risk quarterly or after major change.

| # | Risk | Likelihood | Impact | Mitigation | Owner | Res Risk |
|---|---|---|---|---|---|---|
| 1 | Phishing compromise of user credentials | High | High | MFA, simulated campaigns, email filter (SPF,DKIM,DMARC) | IT Sec Manager | Low |
| 2 | Cloud misconfiguration exposing retail data | High | High | Automated compliance scanner, least-privilege IAM, periodic audits | Cloud Lead | Low |
| 3 | Insider misuse or data exfiltration | High | High | DLP software, access-log analytics, HR screening | CISO / HR | Low |
| 4 | Ransomware infection | Med | Med | Endpoint EDR, immutable backups, patch management | SysAdmin | Low |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | DDoS/Service Outage | Low | High | WAF, CDN, redundant links, test BCP | IT Ops | Low |
| 6 | Unauthorized access to hospital servers | Med | High | Physical access control, CCTV, audit trails | Facilities | Low |

Each risk has a designated owner responsible for monitoring controls and reporting into the monthly security dashboard.

# 5. Mitigation Methods

## 5.1. Technical Controls

- **Next-generation firewall + IDS/IPS**: monitors inbound/outbound traffic in real time (ISO 27002 §13).
- **Encryption**: AES-256 for data at rest; TLS 1.3 for data in transit (NIST SP 800-52 Rev 2).
- **Multi-Factor Authentication (MFA)**: required for all user accounts; app-based rather than SMS.
- **Automated patch management**: weekly checks; critical patches within 48 hours.
- **Endpoint Detection and Response (EDR)**: monitors anomalies and quarantines malware automatically

## 5.2. Organizational Controls

- **Information Security Policy**: outlines acceptable use, access levels, and incident response steps.

- **Security Governance Committee**: cross-functional body (IT, HR, Legal, Ops) meeting monthly to review metrics.

Controls are classified as:

- **Mandatory**: MFA, encryption, firewall/IDS, patching.
- **Recommended**: DLP, CASB, and advanced analytics (dependent on budget)..

## 6. User Rights and Access Control

Access follows the **Principle of Least Privilege** using **Role-Based Access Control (RBAC)**:

| Role | Data Access | System Access | Notes |
|---|---|---|---|
| Doctors Group | Hospital dataset only | On-prem analytics servers | Read/Write to medical tables |
| Retailers Group | Retail dataset only | Cloud tenant (Azure AU-East) | No access to hospital records |
| Executives & PAs | Reports only (aggregated data) | Dashboard via SSO | No raw data |
| IT Admins | Temporary elevated privilege (“break-glass”) | AD + network infra | Logs audited daily |

All access events are recorded in centralized SIEM (Security Information and Event Management). Privileges expire automatically after 30 days unless renewed.

## 7. Password and Authentication Policy

Analyzing patient feedback with AI requires strict adherence to ethical and governance principles. Patient comments must be anonymized to protect confidentiality, with explicit consent obtained where data is identifiable. NLP systems risk embedding bias, for example, misclassifying feedback from minority or non-native speakers, which could disadvantage certain patient groups. Legal frameworks such as the Australian Privacy Act, GDPR, and HIPAA emphasize accountability, requiring that AI outputs remain advisory rather than deterministic. Transparent, bias-aware methods and human oversight are essential to ensure both scientific validity and social responsibility. For ICT-driven R&D, these governance issues are not merely compliance obligations but design principles that shape responsible innovation. Embedding privacy-by-design, explainability, and bias mitigation into sentiment analysis systems will be critical for healthcare adoption.

## 8. Storage Security Controls

Analyzing patient feedback with AI requires strict adherence to ethical and governance principles. Patient comments must be anonymized to protect confidentiality, with explicit consent obtained where data is identifiable. NLP systems risk embedding bias, for example, misclassifying feedback from minority or non-native speakers, which could disadvantage certain patient groups. Legal frameworks such as the Australian Privacy Act, GDPR, and HIPAA emphasize accountability, requiring that AI outputs remain advisory rather than deterministic. Transparent, bias-aware methods and human oversight are essential to ensure both scientific

validity and social responsibility. For ICT-driven R&D, these governance issues are not merely compliance obligations but design principles that shape responsible innovation. Embedding privacy-by-design, explainability, and bias mitigation into sentiment analysis systems will be critical for healthcare adoption.

## 9. Plan of Action (Information Security Management System)

Analyzing patient feedback with AI requires strict adherence to ethical and governance principles. Patient comments must be anonymized to protect confidentiality, with explicit consent obtained where data is identifiable. NLP systems risk embedding bias, for example, misclassifying feedback from minority or non-native speakers, which could disadvantage certain patient groups. Legal frameworks such as the Australian Privacy Act, GDPR, and HIPAA emphasize accountability, requiring that AI outputs remain advisory rather than deterministic. Transparent, bias-aware methods and human oversight are essential to ensure both scientific validity and social responsibility. For ICT-driven R&D, these governance issues are not merely compliance obligations but design principles that shape responsible innovation. Embedding privacy-by-design, explainability, and bias mitigation into sentiment analysis systems will be critical for healthcare adoption.

## 10. Business Continuity Plan (BCP)

Analyzing patient feedback with AI requires strict adherence to ethical and governance principles. Patient comments must be anonymized to protect confidentiality, with explicit consent obtained where data is identifiable. NLP systems risk embedding bias, for example, misclassifying feedback from minority or non-native speakers, which could disadvantage certain patient groups. Legal frameworks such as the Australian Privacy Act, GDPR, and HIPAA

emphasize accountability, requiring that AI outputs remain advisory rather than deterministic. Transparent, bias-aware methods and human oversight are essential to ensure both scientific validity and social responsibility. For ICT-driven R&D, these governance issues are not merely compliance obligations but design principles that shape responsible innovation. Embedding privacy-by-design, explainability, and bias mitigation into sentiment analysis systems will be critical for healthcare adoption.

## 11. Balancing Service Quality and Security

Analyzing patient feedback with AI requires strict adherence to ethical and governance principles. Patient comments must be anonymized to protect confidentiality, with explicit consent obtained where data is identifiable. NLP systems risk embedding bias, for example, misclassifying feedback from minority or non-native speakers, which could disadvantage certain patient groups. Legal frameworks such as the Australian Privacy Act, GDPR, and HIPAA emphasize accountability, requiring that AI outputs remain advisory rather than deterministic. Transparent, bias-aware methods and human oversight are essential to ensure both scientific validity and social responsibility. For ICT-driven R&D, these governance issues are not merely compliance obligations but design principles that shape responsible innovation. Embedding privacy-by-design, explainability, and bias mitigation into sentiment analysis systems will be critical for healthcare adoption.

## 12. Continuous Improvement and Next Steps

Analyzing patient feedback with AI requires strict adherence to ethical and governance principles. Patient comments must be anonymized to protect confidentiality, with explicit consent obtained where data is identifiable. NLP systems risk embedding bias, for example,

misclassifying feedback from minority or non-native speakers, which could disadvantage certain patient groups. Legal frameworks such as the Australian Privacy Act, GDPR, and HIPAA emphasize accountability, requiring that AI outputs remain advisory rather than deterministic. Transparent, bias-aware methods and human oversight are essential to ensure both scientific validity and social responsibility. For ICT-driven R&D, these governance issues are not merely compliance obligations but design principles that shape responsible innovation. Embedding privacy-by-design, explainability, and bias mitigation into sentiment analysis systems will be critical for healthcare adoption.

## 13. Conclusion

This review shows that AI-driven sentiment analysis offers strong technical potential but has yet to bridge the gap between patient experience and business performance in healthcare clinics. Current research demonstrates advances in emotion theory, fine-grained sentiment modeling, and action research for operational improvements, yet consistently fails to correlate sentiment with revenue or retention outcomes. NPS, while convenient, is insufficient as a standalone metric. AI frameworks from education provide conceptual guidance, but their application in healthcare requires adaptation to protect patient data and ensure transparency. This positions AI-driven sentiment analysis as an ICT innovation pathway, aligning technical progress in NLP with the dual goals of improving patient outcomes and enabling sustainable business growth in healthcare clinics.

## 14. Implementation Plan and Timeline

This review shows that AI-driven sentiment analysis offers strong technical potential but has yet to bridge the gap between patient experience and business performance in healthcare clinics. Current research demonstrates advances in emotion theory, fine-grained sentiment modeling, and action research

**Statement of Acknowledgment**

I acknowledge that I have used the following AI tool(s) in the creation of this report:

- OpenAI ChatGPT (GPT-5): Used to assist with outlining, refining structure, improving clarity of academic language, and supporting with APA 7th referencing conventions.

I confirm that the use of the AI tool has been in accordance with the Torrens University Australia Academic Integrity Policy and TUA, Think and MDS's Position Paper on the Use of AI. I confirm that the final output is authored by me and represents my own critical thinking, analysis, and synthesis of sources. I take full responsibility for the final content of this report.

## 15. References

Australian Cyber Security Centre (ACSC). (2023). Essential Eight Maturity Model. https://www.cyber.gov.au/

International Organization for Standardization (ISO). (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. ISO.

International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems. ISO.

International Organization for Standardization (ISO). (2021). ISO/IEC 27017:2021 Code of practice for information security controls for cloud services. ISO.

National Institute of Standards and Technology (NIST). (2023). Special Publication 800-63B: Digital Identity Guidelines. U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2020). Special Publication 800-52 Rev. 2: Guidelines for the Selection and Use of Transport Layer Security (TLS). U.S. Department of Commerce.

OWASP Foundation. (2024). OWASP Top 10: Web Application Security Risks. https://owasp.org/Top10/

Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.

Steinberg, J. (2020). Cybersecurity for Dummies. Wiley.

Sutton, M. (2022). The Complete Guide to Cyber Threats. Springer.

Xiao, Y., Li, C., Thürer, M., Liu, Y., & Qu, T. (2022). *Towards lean automation: Fine-grained sentiment analysis for customer value identification. Computers & Industrial Engineering*, *169*, 108186. https://doi.org/10.1016/j.cie.2022.108186