PROTECTING CRITICAL INFRASTRUCTURE IN HEALTHCARE: LEGAL, SECURITY AND GOVERNANCE RESPONSES TO INTERNAL SABOTAGE IN NIGERIAN HOSPITALS

A Case Study of Diesel Diversion at University College Hospital, Ibadan, with Comparative Notes on LUTH, UITH, and LASUTH

Barrister Adebayo Akinade, dfisn
Deputy President & Chief Executive,
Institute of Security Nigeria
Email: bayoakinade77@gmail.com / bayoakinade@yahoo.co.uk

ABSTRACT

The interception of University College Hospital, Ibadan staff by the hospital's Chief Security Officer for allegedly diverting diesel meant for critical units illustrates a persistent threat to healthcare continuity in Nigeria: internal sabotage of essential services. Similar vulnerabilities have been documented at Lagos University Teaching Hospital, University of Ilorin Teaching Hospital, and Lagos State University Teaching Hospital. This paper analyzes the incidents as breaches of legal, ethical, and operational standards in healthcare security management. It examines the roles and responsibilities of hospital security departments, statutory obligations under Nigerian law, and comparative practices in the Commonwealth, United States, United Kingdom, and selected Asian states. Drawing on theories of organizational deviance, risk management, and public trust, the paper applies a philosophical-conceptual framework to explain the causes and consequences of internal sabotage. Findings show that weak inventory controls, poor staff vetting, and inadequate oversight create vulnerabilities that endanger patient safety across Nigeria's tertiary hospitals. The paper recommends integrated security governance, forensic auditing, technological monitoring, and ethical reorientation of healthcare security personnel. It argues that protecting critical hospital infrastructure requires a fusion of law, management, and security culture aligned with international best practices.

Keywords: Healthcare security, Internal sabotage, Diesel diversion, UCH Ibadan, LUTH, UITH, LASUTH, Critical infrastructure, Hospital governance, Nigerian law, Patient safety, Risk management.

1. INTRODUCTION

Healthcare institutions are classified as critical infrastructure because their failure directly endangers human life. The incident at University College Hospital, Ibadan, where staff were caught diverting diesel intended for generators serving ICU, theatre, and emergency units, represents more than theft. It is a breach of the duty of care owed to patients, a violation of public trust, and a potential act of criminal negligence.

Comparable issues of asset diversion and supply chain fraud have been reported in Lagos University Teaching Hospital, University of Ilorin Teaching Hospital, and Lagos State University Teaching Hospital, indicating a systemic challenge across Nigeria's tertiary health system.

This paper uses these cases as a lens to analyze systemic weaknesses in healthcare security across Nigeria. It examines the legal framework governing healthcare institutions, the operational procedures expected of security departments, and the ethical standards required of personnel. The objective is to produce a position paper that informs policy, guides reform, and strengthens the integrity of hospital security systems in Nigeria and comparable jurisdictions.

2. BACKGROUND INFORMATION

2.1 The Incidents

Video evidence circulating via Intel Region and WhatsApp shows UCH Ibadan staff intercepted by the Chief Security Officer while diverting diesel from hospital storage. The diesel was designated for generators powering life-support systems during national grid failures.

Internal audits and media reports from LUTH, UITH, and LASUTH between 2018 and 2024 have also flagged discrepancies in fuel consumption, pharmaceutical stock, and medical equipment, suggesting recurring internal threats.

2.2 Context of Healthcare Infrastructure in Nigeria

Nigeria's public hospitals face chronic underfunding, erratic power supply, and reliance on diesel generators. This creates high-value targets for diversion and fraud. Internal theft of fuel, drugs, and equipment is a documented challenge in tertiary hospitals nationwide.

3. HISTORICAL BACKGROUND AND PREAMBLE

From the 1980s, Nigerian teaching hospitals adopted generator-dependent power models due to grid instability. Early security departments focused on access control and crowd management. The rise of sophisticated fraud and supply chain manipulation from the 2000s necessitated a shift toward asset protection, forensic accounting, and internal investigation functions.

Historically, hospital security was treated as low-skilled guarding. The trend globally and in Nigeria is toward professionalization, with CSOs required to understand risk assessment, legal procedure, and healthcare-specific vulnerabilities.

4. OVERVIEW OF THE SUBJECT MATTER

The subject matter concerns the protection of critical operational assets in hospitals against internal threats. It covers:
1. Legal classification of diesel diversion as theft, sabotage, and potential endangerment.
2. Roles of the Chief Security Officer and hospital management in detection, response, and prosecution.
3. Procedural safeguards required in procurement, storage, and consumption of fuel.
4. Ethical and professional standards for healthcare security personnel.
5. Comparative lessons from other jurisdictions on preventing internal sabotage.

5. LITERATURE REVIEW

5.1 Healthcare Security and Internal Threats
The International Association for Healthcare Security and Safety identifies employees as the leading source of internal theft in hospitals. Akinade, in Security, Legal Safety Issues in Healthcare Institutions, argues that Nigerian hospitals underinvest in supply chain integrity and staff integrity screening, creating predictable fraud patterns observed in UCH, LUTH, UITH, and LASUTH.

5.2 Organizational Deviance and Trust
Ashforth and Anand's theory of normalization of corruption explains how small thefts become institutionalized when undetected. Akinade links this to the erosion of public trust in public hospitals, which accelerates privatization and inequality in healthcare access.

5.3 Risk Management and Critical Infrastructure Protection
ISO 22301 and Nigeria's Critical National Infrastructure Policy frame hospitals as essential services requiring layered protection. Akinade emphasizes that risk management in hospitals must integrate physical security, process controls, and personnel vetting.

6. PHILOSOPHICAL AND CONCEPTUAL FRAMEWORK

6.1 Duty of Care and Professional Ethics
Derived from medical jurisprudence and common law, the duty of care requires healthcare providers to avoid acts that foreseeably harm patients. Diesel diversion breaches this duty by risking treatment interruption.

6.2 Social Contract and Public Trust
Public hospitals operate under a social contract: citizens fund them through taxation and expect safe services. Internal sabotage violates this contract and delegitimizes the state.

6.3 Deterrence and Proportionality

Classical criminology suggests that certainty and swiftness of sanction deter misconduct more than severity. Akinade applies this to hospital fraud, arguing for predictable investigation and disciplinary processes.

7. PROCESSES AND PROCEDURES IN HEALTHCARE INSTITUTIONS

7.1 Procurement and Storage

- Centralized procurement with dual authorization.
- Metered dispensing systems linked to generator run-time logs.
- Segregation of duties between procurement, stores, and finance.

7.2 Monitoring and Detection

- CCTV and RFID tagging of fuel tanks.
- Daily reconciliation of fuel levels by independent staff.
- Whistleblower channels protected under the Whistleblower Protection Policy.

7.3 Response and Investigation

- Immediate containment by CSO.
- Preservation of evidence for police investigation.
- Internal disciplinary committee in parallel with criminal process.

8. ROLES AND RESPONSIBILITIES OF SECURITY DEPARTMENT AND PERSONNEL

8.1 Chief Security Officer

- Conduct risk assessments of critical assets.
- Supervise access to fuel and pharmaceutical stores.
- Liaise with police and EFCC on criminal matters.
- Report directly to the hospital CMD on security breaches.

8.2 Security Personnel

- Maintain access logs and patrol records.
- Conduct integrity checks on staff entering restricted areas.
- Undergo mandatory training on healthcare ethics and legal limits of force.

8.3 Hospital Management

- Provide resources for security infrastructure.
- Enforce zero-tolerance policy on diversion and fraud.
- Ensure disciplinary actions are non-discriminatory and evidence-based.

9. STATUTORY PROVISIONS, LEGISLATION AND CONSTITUTIONAL REQUIREMENTS

9.1 Criminal Code Act, Cap C38 LFN 2004

Sec. 390 defines stealing. Sec. 516 criminalizes conspiracy. Sec. 247-249 address negligent acts endangering life.

9.2 Miscellaneous Offences Act, Cap M17 LFN 2004

Sec. 1 criminalizes sabotage of essential services, including hospitals.

9.3 Corrupt Practices and Other Related Offences Act 2000

Covers diversion of public resources by public officers.

9.4 Constitution of the Federal Republic of Nigeria 1999

Sec. 33 guarantees right to life. Sec. 14(2)(b) places security and welfare as primary government purpose, extending to public hospitals.

9.5 National Health Act 2014

Sec. 7 imposes obligations on tertiary hospitals to maintain minimum standards, including power backup systems.

10. COMPARATIVE INSIGHTS

10.1 United Kingdom and England

NHS Trusts operate under the NHS Counter Fraud Authority. All hospitals use electronic fuel management and mandatory fraud risk assessments. The Fraud Act 2006 criminalizes diversion of public assets. Staff are subject to professional sanctions by the Nursing and Midwifery Council.

10.2 United States

Hospitals are covered under the Health Insurance Portability and Accountability Act and Joint Commission standards, which require asset protection plans. The False Claims Act allows civil penalties for diversion of federal-funded resources. FBI and HHS-OIG investigate internal fraud.

10.3 Canada

Provincial health authorities use Public Sector Accounting Standards for inventory control. The Criminal Code Sec. 380 addresses fraud, and provincial colleges discipline health workers for conduct endangering patients.

10.4 Commonwealth and Asian Countries

India’s Clinical Establishments Act mandates security audits. Singapore’s hospitals use centralized automated fuel systems with real-time alerts. Malaysia’s MOH enforces the Whistleblower Protection Act 2010 in public hospitals.

11. PROSPECTS, INNOVATIONS AND RECOMMENDATIONS

11.1 Technological Innovation

- Install IoT fuel sensors with real-time alerts to CSO and CMD.
- Use AI-driven anomaly detection on supply chain data.
- Integrate CCTV with access control for fuel stores.

11.2 Governance Reform

- Adopt ISO 22301 Business Continuity Management in all teaching hospitals.
- Establish independent Audit and Risk Committees with external members.
- Extend mandatory reporting and audit standards to LUTH, UITH, LASUTH, and all federal and state teaching hospitals.

11.3 Personnel and Integrity Management

- Mandatory integrity vetting for staff handling critical assets.
- Annual ethics training linked to license renewal for health workers.
- Implement code of conduct with clear sanctions for diversion.

11.4 Motivation and Professionalism

- Link performance bonuses to patient safety metrics, not just attendance.
- Professionalize hospital security through certification with ISN and IAHSS.
- Create career progression for security personnel to reduce bribe-seeking behavior.

12. CONCLUSION

The UCH diesel diversion case, alongside similar incidents in LUTH, UITH, and LASUTH, is a warning: hospitals cannot separate clinical safety from physical and supply chain security. Internal sabotage thrives where controls are weak, accountability is absent, and professional standards are unenforced.

Protecting critical healthcare infrastructure requires a tripartite approach: robust legal enforcement, technologically-enabled monitoring, and a culture of integrity among staff. Nigeria must professionalize hospital security across all teaching hospitals, align it with international standards, and treat attacks on hospital operations as attacks on the right to life itself.

13. REFERENCES AND FURTHER READING

1. Akinade, A. Security, Legal Safety Issues in Healthcare Institutions. Lagos: ISN Press, 2010.
2. Akinade, A. Contemporary Security Issues on Governance and Statecraft. Lagos: ISN Press, 2018.
3. Akinade, A. Managing Strategic Security in Statecraft, Public Affairs and Foreign Relations. Lagos: ISN Press, 2019.
4. Akinade, A. Community Policing: Strategic Approaches in Crime Prevention. Lagos: ISN Press, 2018.
5. Akinade, A. Security Operations, Crime Prevention and Good Governance. Lagos: ISN Press, 2007.
6. Federal Republic of Nigeria. Criminal Code Act, Cap C38 LFN 2004.
7. Federal Republic of Nigeria. Miscellaneous Offences Act, Cap M17 LFN 2004.

8. Federal Republic of Nigeria. Corrupt Practices and Other Related Offences Act 2000.
9. Federal Republic of Nigeria. National Health Act 2014.
10. Federal Republic of Nigeria. Constitution of the Federal Republic of Nigeria 1999, as amended.
11. International Association for Healthcare Security and Safety. Healthcare Security Fundamentals, 2022.
12. ISO. ISO 22301:2019 Societal Security – Business Continuity Management Systems.
13. NHS Counter Fraud Authority. Fraud and Corruption in the NHS, 2023.
14. Ashforth, B.E. & Anand, V. "The Normalization of Corruption in Organizations." Research in Organizational Behavior, 2003.
15. U.S. Department of Health and Human Services OIG. Compliance Program Guidance for Hospitals, 2021.
16. Singapore Ministry of Health. Hospital Security and Asset Protection Guidelines, 2020.

Barrister Adebayo Akinade, dfisn
Deputy President & Chief Executive
Institute of Security Nigeria