

South Africa's AI & Cybersecurity Leadership: From POPIA to Advanced Industry Standards

From Data Protection to Cyber Resilience: Evaluating a Standards-Led Model for Responsible AI

June 2, 2026

Erich Barlow, MIS, CITP, FBCS

Abstract

South Africa has emerged as one of the continent's most institutionally mature jurisdictions for governing data, cybersecurity, and emerging AI systems. Its leadership rests less on a single "AI law" than on an interlocking governance stack: constitutional privacy protections, the Protection of Personal Information Act (POPIA), the Cybercrimes Act, sector regulation in finance, and a developing national AI policy framework (Department of Communications and Digital Technologies [DCDT], 2024; Republic of South Africa, 2021). Together, these instruments create a relatively credible basis for responsible innovation in data-intensive sectors such as finance, energy, and healthcare. POPIA is now materially enforced: the Information Regulator reported 1,044 public complaints in 2023/24, resolved 637 of them, and assessed 13 responsible parties for POPIA compliance, while also scaling outreach and digital compliance services (Information Regulator South Africa, 2024). South Africa has also moved beyond generic cyber hygiene in finance by publishing Joint Standard 2 of 2024 on cybersecurity and cyber resilience for financial institutions (Financial Sector Conduct Authority [FSCA] & Prudential Authority [PA], 2024). In parallel, the 2024 National AI Policy Framework signals a human-centered, risk-based approach to future AI governance (DCDT, 2024).

This paper argues that South Africa's model is strongest where legal obligations, supervisory capacity, and sector-specific controls align; it is weaker where enforcement bandwidth, digital inequality, and critical-infrastructure resilience constrain implementation. The central policy implication is that South Africa's comparative advantage lies not in deregulated AI adoption, but in coupling innovation with accountable

data governance, cyber resilience, and standards-led implementation. That combination is particularly relevant for finance, energy, and healthcare, where systemic trust and service continuity are non-negotiable (Eskom Holdings SOC Ltd., 2024; FSCA & PA, 2024; Information Regulator South Africa, 2024).

Table of Contents

Abstract	1
Introduction	4
Background & Literature Review	4
Methodology / Analytical Framework	6
Key Findings & Analysis	6
Table 1. Sector comparison: governance maturity and implementation posture	9
Risk, Security, & Governance Implications	10
Practical Use Cases / Case Studies	11
Case Study 1: Finance — regulatory hardening as an enabler of secure digital finance..	11
Case Study 2: Healthcare — privacy obligations outpacing cyber-operational readiness	11
Case Study 3: Energy — governance without equal public standardization	11
Recommendations	12
Priority 1: Establish sector-specific AI assurance profiles for finance, energy, and healthcare	12
Priority 2: Treat third-party and operator risk as a first-order control domain	12
Priority 3: Expand healthcare cyber modernization beyond privacy compliance	12
Priority 4: Create a critical-infrastructure cyber standardization pathway for energy	12
Priority 5: Build supervisory interoperability across privacy, cyber, and AI	13
Limitations & Assumptions	13
Conclusion	13
References	15

Introduction

The policy problem is not whether South Africa should pursue AI-enabled transformation, but whether it can do so without undermining privacy, operational resilience, and public trust in critical sectors. In finance, AI and digitization amplify both inclusion opportunities and systemic cyber risk. In healthcare, digitization improves care coordination but concentrates on highly sensitive personal and health data. In energy, digital modernization of grid and generation environments can improve performance while increasing exposure to cyber-physical disruption. A credible leadership position therefore depends on whether governance mechanisms convert legal principles into operational control.

South Africa is significant because it already possesses several governance ingredients many jurisdictions still lack: a comprehensive data protection statute enforced since July 1, 2021; cybercrime legislation in force since December 1, 2021; an active Information Regulator; sector-specific financial cyber standards published in 2024; and a draft national AI framework published in October 2024 (DCDT, 2024; FSCA & PA, 2024; Information Regulator South Africa, 2024; Republic of South Africa, 2021). The result is an emerging, layered governance architecture rather than a single omnibus AI regime. This is more pragmatic than it first appears, but it also creates fragmentation risk if standards, supervisory expectations, and incident reporting remain misaligned across sectors.

The significance of this case extends beyond South Africa. Many African states are simultaneously pursuing digital transformation, financial inclusion, health modernization, and energy transition, often without mature regulatory capacity. South Africa's experience suggests that responsible innovation is more likely where data protection, cyber resilience, and sector governance are treated as enabling infrastructure rather than as post hoc compliance burdens. That does not make South Africa a frictionless model; rather, it makes it a useful test case in balancing innovation with constitutional rights, accountability, and critical-service continuity.

Background & Literature Review

South Africa's governance baseline begins with POPIA, which operationalizes the constitutional right to privacy through conditions for lawful processing, security safeguards, breach notification, and supervisory oversight by the Information Regulator. POPIA's practical importance is not merely doctrinal. In 2023/24, the Information Regulator reported that its enforcement efforts "gathered momentum," received 1,044 complaints from the public, resolved 637, and assessed 13 responsible parties for POPIA compliance (Information Regulator South Africa, 2024). The Regulator also expanded public awareness

and educational activity, suggesting that compliance culture is being built through both enforcement and outreach (Information Regulator South Africa, 2024).

Cybersecurity governance rests on a broader legislative layer. The Cybercrimes Act 19 of 2020 criminalizes unlawful access, interception, interference, cyber fraud, cyber extortion, and related acts, while also providing investigative powers, mutual assistance provisions, a designated point of contact, and reporting obligations for electronic communications service providers and financial institutions (Republic of South Africa, 2021). Importantly, the Act does not function as a general security-management framework; it is stronger on criminalization and law-enforcement powers than on sectoral resilience engineering. This distinction matters because criminal law deters and punishes, but it does not by itself ensure resilience in hospitals, payment systems, or generation environments.

The most advanced sector-specific cyber instrument appears in finance. In May 2024, the Prudential Authority and Financial Sector Conduct Authority published Joint Standard 2 of 2024 on cybersecurity and cyber resilience (FSCA & PA, 2024). The standard covers governance, cyber strategy, cyber-resilience fundamentals, cyber hygiene, and notification/reporting obligations for financial institutions (FSCA & PA, 2024). This is a notable step because it moves the sector from broad expectations to prescriptive supervisory architecture, including board and management responsibilities and expectations for testing and control effectiveness. Finance therefore offers the clearest example of South Africa shifting from policy intent to regulated operational resilience.

AI governance is newer and less legally mature. The Department of Communications and Digital Technologies published the South Africa National AI Policy Framework on October 25, 2024, as a foundational instrument to guide subsequent policy and possible legislation (DCDT, 2024). Public descriptions of the framework emphasize human-centered AI, privacy and data protection, safety and security, transparency and explainability, fairness and bias mitigation, talent development, infrastructure, and public-sector implementation (DCDT, 2024; OECD.AI, 2026). This aligns South Africa with a risk-based and rights-aware policy trajectory, but at present it remains a framework rather than a binding AI statute. Therefore, any claim that South Africa already has comprehensive AI regulation would be overstated. Confidence on the direction of travel is high; confidence in the final legal design is lower because the framework remains part of a policy-development process.

Sector-specific literature reinforces the need for layered controls. In healthcare, legal analysis notes that POPIA must be interpreted together with the National Health Act and Health Professions Council of South Africa (HPCSA) confidentiality guidelines, particularly because health information is exceptionally sensitive and may trigger both privacy and professional-conduct obligations (Health Professions Council of South Africa [HPCSA],

n.d.; Werksmans Attorneys, 2023). In energy, Eskom’s integrated reporting shows that operational disruption remains a material strategic concern and that governance and risk reporting are central to utility resilience, even if public reporting is not a detailed cyber technical disclosure (Eskom Holdings SOC Ltd., 2024). In cyber threat studies, a South African survey by CSIR found that 88% of respondents had suffered a security breach in the previous 12 months, 90% of those were targeted multiple times, and the top reported root cause was third-party connectivity at 48% (Council for Scientific and Industrial Research [CSIR], 2024). These findings suggest that third-party risk, identity controls, and resilience engineering remain central across sectors.

Methodology / Analytical Framework

This white paper uses a governance-capability-resilience framework. First, it assesses governance maturity: whether legal obligations are explicit, sector-relevant, and supervised. Second, it evaluates capability maturity: whether institutions have the operational means to implement governance through controls, reporting, and assurance. Third, it examines resilience maturity: whether sectors can absorb, respond to, and recover from cyber incidents while preserving trust, continuity, and legal compliance. The focus is evidence from the last three to five years, with priority given to official instruments, annual reports, regulatory publications, and public-sector documentation.

Analytically, the paper distinguishes between three categories of claim:

1. **Evidence:** directly supported by official reports, statutes, or public supervisory documents.
2. **Inference:** conclusions drawn by comparing instruments across sectors.
3. **Opinion:** normative recommendations on priorities or sequencing.

This distinction matters because South Africa’s AI governance remains partly prospective, whereas POPIA enforcement and financial cyber regulation are already observable. Accordingly, the strongest claims in this paper concern privacy enforcement and financial-sector cyber governance; claims about AI leadership are better framed as “emerging leadership through policy design” than as settled regulatory dominance.

Key Findings & Analysis

Finding 1: South Africa’s strongest comparative advantage is its layered governance stack, not a single “AI law.”

South Africa's governance strength derives from combining POPIA, the Cybercrimes Act, sector regulation, and a national AI policy process. POPIA creates accountability for personal information processing and breach notification; the Cybercrimes Act addresses criminal conduct and investigative powers; Joint Standard 2 of 2024 creates a sector-specific cyber-resilience regime in finance; and the AI Policy Framework provides a human-centered roadmap for future AI governance. This layered approach is more realistic for critical sectors than waiting for a single AI statute.

The trade-off is fragmentation. Layered governance works only if reporting obligations, technical standards, sector supervisors, and procurement practices are coherent. Without that coherence, organizations can become "compliant" on paper while remaining operationally brittle. That risk is especially acute where vendors, cloud services, and AI systems cut across multiple regulatory domains. The CSIR survey's finding that 48% of breaches were attributed to third-party connections supports the argument that governance maturity must extend beyond entity boundaries to ecosystems and supply chains (CSIR, 2024).

Finding 2: POPIA has moved from symbolic legislation to consequential supervisory infrastructure.

The Information Regulator's 2023/24 annual report shows meaningful supervisory activity: 1,044 complaints received, 637 resolved, 13 responsible parties assessed for POPIA compliance, and a budget increase to R107.953 million from R100.609 million (Information Regulator South Africa, 2024). The Regulator also launched or expanded digital service channels, including an eServices portal published in 2024 to streamline compliance interactions (Information Regulator South Africa, 2024). These facts indicate that South Africa is building the institutional machinery needed for scalable oversight, even if enforcement capacity remains finite relative to the economy-wide attack surface.

A practical implication follows: POPIA is now material to enterprise risk, board governance, and incident response. This is particularly relevant in healthcare and finance, where data sensitivity and supervisory scrutiny are high. The assumption that privacy law is a secondary legal issue, separate from cyber resilience, is no longer defensible. In South Africa, privacy governance increasingly functions as a resilience control because breach notification, operator management, and security safeguards directly influence crisis outcomes.

Finding 3: Finance is the most mature sectoral model for secure, responsible innovation.

Finance is the clearest example of South Africa translating high-level cyber principles into measurable regulatory expectations. Joint Standard 2 of 2024 establishes requirements for governance, strategy, cyber-resilience fundamentals, hygiene practices, and incident reporting for financial institutions (FSCA & PA, 2024). In effect, finance now has a more advanced control architecture than the broader economy. This matters because financial systems are both highly digitized and systemically interconnected; a cyber incident can cascade across institutions and undermine trust at national scale.

For AI adoption, this sectoral maturity is an advantage. AI-enabled fraud detection, credit operations, customer analytics, and operational automation can be deployed within a stronger risk-management perimeter than in less regulated sectors. The trade-off is cost. Smaller institutions may experience compliance burden, and rigid supervisory expectations can slow experimentation. However, that cost may be economically justified if it reduces systemic risk, enforcement exposure, and customer-trust erosion. The better interpretation is that South Africa's financial model supports "secure innovation," not innovation at any price.

Finding 4: Healthcare has a strong normative privacy base but weaker demonstrated cyber-operational maturity.

Healthcare information in South Africa is governed through overlapping duties under POPIA, the National Health Act, and HPCSA confidentiality guidance (HPCSA, n.d.; Werksmans Attorneys, 2023). This creates a relatively strong rights-based basis for protecting patient information. Legal commentary further emphasizes that healthcare providers and their operators must manage confidentiality, consent, retention, and security safeguards with particular care, and that non-compliance can attract both POPIA sanctions and professional consequences (Werksmans Attorneys, 2023).

Operationally, however, available evidence suggests that healthcare remains exposed. A 2024 University of Johannesburg study reviewing incidents involving major South African healthcare organizations identified outdated IT systems, insufficient cybersecurity protocols, inadequate staff training, and weak business continuity planning as recurring problems (Ngoasheng, 2024). This does not negate South Africa's governance leadership; it shows the gap between legal obligation and operational execution. In healthcare, South Africa is a model for normative governance design, but not yet consistently for cyber-resilient execution. Confidence in this conclusion is moderate because the evidence base is narrower and more incident-driven than in finance.

Finding 5: Energy governance is strategically important but comparatively under-standardized in public view.

Energy is central because cyber incidents can become public-safety, economic, and national-stability events. Eskom’s 2024 integrated report documents a difficult operating environment, including 329 days of loadshedding in the reporting year, R33.9 billion in spend on Eskom and IPP OCGTs to mitigate loadshedding, and an increasingly formalized approach to risk, resilience, and governance reporting (Eskom Holdings SOC Ltd., 2024). These data points do not prove specific cyber weakness, but they do show why cyber resilience in energy should be treated as critical infrastructure governance, not simply enterprise IT.

The gap relative to finance is visibility and sector-specific standardization. Publicly visible energy governance emphasizes enterprise risk and operational resilience, but there is no equivalent in the current evidence set to Joint Standard 2 of 2024 for the energy sector. That means South Africa’s “model” status in energy is presently more inferential: it has the legal primitives and institutional need, but less publicly evidenced sector-specific cyber codification. This is a strategic vulnerability because energy disruptions have economy-wide spillovers that can overwhelm purely entity-level governance.

Table 1. Sector comparison: governance maturity and implementation posture

Sector	Primary governance instruments	Evidence of maturity	Main strengths	Main gaps
Finance	POPIA; Cybercrimes Act; Joint Standard 2 of 2024	Sector-specific cyber standard; supervisory reporting obligations	Highest visible regulatory maturity; clearer board and control expectations	Compliance cost; potential burden on smaller firms
Healthcare	POPIA; National Health Act; HPCSA guidance	Strong confidentiality and privacy obligations	Strong rights-based framework for sensitive data	Legacy systems; uneven business continuity and cyber execution
Energy	POPIA; Cybercrimes Act; enterprise	Criticality recognized	National strategic importance; governance	Less visible sector-specific cyber

Sector	Primary governance instruments	Evidence of maturity	Main strengths	Main gaps
	risk/governance reporting	through resilience reporting	attention at enterprise level	standardization in public evidence

Risk, Security, & Governance Implications

The central governance implication is that South Africa’s leadership depends on implementation discipline, not legislative proliferation. More laws will not automatically produce more resilience. The stronger move is to align existing legal duties with sector-specific control baselines, third-party oversight, incident reporting, and board accountability. This is especially important because breach causation in South Africa appears strongly linked to ecosystem risk: third-party connectivity was identified by CSIR respondents as the top breach source at 48%, ahead of phishing at 45% (CSIR, 2024).

A second implication concerns trust in economics. In sectors like finance and healthcare, the cost of trust failure often exceeds the cost of preventive controls because trust erosion can trigger customer attrition, regulatory scrutiny, litigation, and operational disruption simultaneously. South Africa’s regulatory posture increasingly reflects this logic. POPIA’s enforcement trajectory, the Information Regulator’s caseload, and the financial sector’s joint cyber standard all indicate that trust and compliance are becoming measurable governance assets rather than abstract ethical preferences (FSCA & PA, 2024; Information Regulator South Africa, 2024).

A third implication concerns AI specifically. AI governance in South Africa will be credible only if it is operationalized through the same disciplines that now shape privacy and cyber resilience: data lineage, model accountability, third-party risk management, human oversight in high-impact decisions, and incident response. The 2024 AI Policy Framework points in this direction through its emphasis on privacy, security, fairness, transparency, and public-sector implementation (DCDT, 2024; OECD.AI, 2026). But until those principles translate into sectoral standards, procurement rules, and assurance practices, AI leadership remains emerging rather than fully institutionalized.

Practical Use Cases / Case Studies

Case Study 1: Finance — regulatory hardening as an enabler of secure digital finance

The publication of Joint Standard 2 of 2024 is a case of regulatory hardening in a highly digitized sector (FSCA & PA, 2024). It shows how a jurisdiction can shift from general cyber expectations to enforceable expectations around governance, hygiene, resilience, and reporting. For AI-enabled financial services, this provides a controlled environment for adopting tools such as fraud analytics, risk scoring, and operational automation while maintaining stronger supervisory assurance. The model is transferable: sectors facing systemic interdependence should not rely on generic cyber guidance alone.

Case Study 2: Healthcare — privacy obligations outpacing cyber-operational readiness

Healthcare illustrates a different dynamic. South Africa has a relatively robust legal-ethical regime for health information through POPIA, the National Health Act, and HPCSA guidance (HPCSA, n.d.; Werksmans Attorneys, 2023). Yet evidence from incident analysis and academic reviews suggest operational weaknesses persist, including outdated systems and insufficient business continuity planning (Ngoasheng, 2024). The lesson is that sectoral trust cannot be sustained by consent forms and confidentiality rules alone; it requires cyber-operational modernization, secure architectures, and tested recovery capability.

Case Study 3: Energy — governance without equal public standardization

Eskom's reporting demonstrates mature enterprise governance and clear acknowledgment of operational and resilience risks in a national critical infrastructure environment (Eskom Holdings SOC Ltd., 2024). However, compared with finance, the publicly visible cyber-regulatory codification appears less developed. The lesson is that critical infrastructure sectors cannot rely on enterprise disclosure and general law alone; they benefit from sector-specific resilience standards, incident coordination expectations, and supply-chain assurance mechanisms.

Recommendations

Priority 1: Establish sector-specific AI assurance profiles for finance, energy, and healthcare

South Africa should not wait for a comprehensive AI Act before acting. It should develop sector-specific AI assurance profiles that map existing obligations under POPIA, cyber rules, and sector governance to concrete requirements for model risk, data quality, explainability, human oversight, third-party controls, and incident escalation. Finance can lead because its cyber governance is already more mature.

Priority 2: Treat third-party and operator risk as a first-order control domain

Given the evidence that third-party connectivity is a major breach source, South African organizations should require stronger contractual controls, audit rights, segregation, secure integration patterns, and breach-notification service levels for operators and suppliers. POPIA compliance should be tied to technical assurance, not only contractual wording.

Priority 3: Expand healthcare cyber modernization beyond privacy compliance

Healthcare needs targeted investment in identity security, backup integrity, network segmentation, secure EHR integration, and tested business continuity. POPIA and confidentiality rules should be treated as governance prerequisites, not as substitutes for cyber resilience. A minimum healthcare cyber baseline, aligned with patient safety and continuity, would close a material implementation gap.

Priority 4: Create a critical-infrastructure cyber standardization pathway for energy

Energy should move toward the same degree of public standardization now visible in finance, adapted for OT/ICS realities. At minimum, this should include governance expectations, supplier assurance, incident coordination, recovery testing, and security requirements for digital modernization programs.

Priority 5: Build supervisory interoperability across privacy, cyber, and AI

South Africa's layered model is an advantage only if supervisory interfaces are coherent. A practical step is to align incident taxonomies, reporting thresholds, and assurance expectations across privacy, financial cyber supervision, and future AI governance so that enterprises are not forced into fragmented compliance silos.

Limitations & Assumptions

This paper prioritizes official and recent public evidence, which creates three limitations. First, public reporting on energy-sector cyber controls is less granular than reporting in finance, so conclusions on energy are partly inferential (Eskom Holdings SOC Ltd., 2024; FSCA & PA, 2024). Second, South Africa's AI policy remains emergent; the 2024 framework is a strong directional indicator but not yet a complete statutory regime (DCDT, 2024; OECD.AI, 2026). Third, some sector-specific implementation evidence, especially in healthcare, is incident-driven or academic rather than published through uniform supervisory reporting, which reduces comparability (Ngoasheng, 2024). Confidence is high for claims about POPIA enforcement and financial cyber regulation; moderate for healthcare-operational conclusions; and moderate-to-lower for claims about energy cyber standardization and final AI regulatory design.

An additional assumption is that responsible innovation should be evaluated not only by innovation output but by trust preservation, continuity, and rights protection. Some market-oriented perspectives would argue that stronger regulation slows AI uptake. That argument is plausible in the short term. However, in critical sectors, under-governed innovation can create delayed costs that are larger than early compliance costs, especially where outages, data compromise, or discriminatory automated decisions damage system legitimacy. This paper therefore adopts a resilience-first view of innovation economics.

Conclusion

South Africa's leadership in AI and cybersecurity is real, but it is best understood as institutional leadership through governance layering, not as leadership through a single dominant AI statute. POPIA provides a meaningful accountability backbone; the Cybercrimes Act supplies criminal-law and investigative structure; financial regulators have advanced the most concrete cyber-resilience standard; and the national AI policy process signals a human-centered, risk-based path for future AI governance (DCDT, 2024;

FSCA & PA, 2024; Information Regulator South Africa, 2024; Republic of South Africa, 2021). This combination gives South Africa a stronger basis for responsible innovation than many peer jurisdictions.

The harder question is implementation. Finance demonstrates that South Africa can convert governance intent into operational expectations (FSCA & PA, 2024). Healthcare shows that strong privacy norms do not guarantee resilient execution (Ngoasheng, 2024; Werksmans Attorneys, 2023). Energy demonstrates the urgency of extending standards-led resilience to critical infrastructure with systemic consequences (Eskom Holdings SOC Ltd., 2024). If South Africa closes those implementation gaps—especially around third-party risk, sector-specific assurance, and interoperability across privacy, cyber, and AI oversight—it can credibly serve as a continental model for trusted digital transformation. If it does not, its leadership will remain strongest in policy design and weaker in execution. That is the central strategic trade-off.

References

Council for Scientific and Industrial Research. (2024). *Data breaches in South Africa: Survey report*.

https://www.csir.co.za/sites/default/files/Documents/241013_CSIR%20Infographic%20posters_Draft%204_Data%20breaches.pdf

Department of Communications and Digital Technologies. (2024, October 25). *South Africa national AI policy framework*. <https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html>

Eskom Holdings SOC Ltd. (2024). *Integrated report for the year ended 31 March 2024*. <https://www.eskom.co.za/wp-content/uploads/2024/12/Eskom-integrated-report-2024.pdf>

Financial Sector Conduct Authority & Prudential Authority. (2024, May 17). *Joint Communication 2 of 2024: Publication of the Joint Standard – Cybersecurity and cyber resilience*. <https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2024/Joint-Communication-2-of-2024-Publication-of-the-Joint-Standard-Cybersecurity-and-cyber-resilience>

Financial Sector Conduct Authority & Prudential Authority. (2024). *Joint Standard 2 of 2024: Cybersecurity and cyber resilience requirements for financial institutions*. https://jutacomplnews.co.za/media/filestore/2025/01/Joint_standard_2_cybersecurity.pdf

Health Professions Council of South Africa. (n.d.). *PAIA & POPIA manuals*. <https://www.hpcsacsa.co.za/page/paia-popia>

Health Professions Council of South Africa. (2023, June 15). *HPCSA POPIA manual*. <https://www.hpcsacsa-blogs.co.za/hpcsacsa-popia-manual/>

Information Regulator (South Africa). (2024). *Annual report 2023/24*. <https://www.inforegulator.org.za/wp-content/uploads/2025/05/Information-Regulator-Annual-Report-2024-Final-06-October-2024.pdf>

Ngoasheng, A. (2024). *Cybersecurity attacks and business continuity in South Africa's healthcare sector* (Master's thesis, University of Johannesburg). <https://ujcontent.uj.ac.za/esploro/outputs/graduate/Cybersecurity-attacks-and-business-continuity-in/9957596407691>

OECD.AI. (2026). *South Africa national artificial intelligence policy framework*.
<https://oecd.ai/en/dashboards/policy-initiatives/south-africa-national-artificial-intelligence-policy-framework>

Republic of South Africa. (2021). *Cybercrimes Act 19 of 2020*.
https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

Werksmans Attorneys. (2023, June 7). *The legal and ethical processing of healthcare information*. <https://werksmans.com/the-legal-and-ethical-processing-of-healthcare-information/>