

External review: Information governance and confidentiality practices at the King Edward VII Memorial Hospital, Falkland Islands

“Every person has the right to respect for his or her private and family life, his or her home and his or her correspondence and, except with his or her own consent, no person shall be subjected to the search of his or her person or property or the entry by others on his or her premises.”

Falkland Islands Constitution Order 2008

“Every citizen should feel confident that information about their health is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the health and social care system should see information governance as part of their responsibility.”

Dame Fiona Caldicott. The Information Governance Review, March 2013

Executive summary

This independent external review examines how the King Edward VII Memorial Hospital (KEMH) and the Falkland Islands Government (FIG) responded to two significant data breaches in 2019 and 2022. It also assesses the current maturity of information governance and confidentiality practices across the Directorate of Health and Social Care in Falkland Islands.

The review was commissioned following a Supreme Court Consent Order and is based on extensive document analysis, interviews, focus groups, surveys, and site visits. It provides an objective baseline for improvement and a clear set of practical recommendations.

The information breaches happened when two separate non-clinical support staff were found to have accessed electronic patient records, without a clear justifiable reason or purpose.

These incidents caused substantial distress, loss of trust, and long-lasting concern within the community, amplified by the small-island context where personal relationships and social proximity heighten the impact of confidentiality failures.

Findings from the look-back review (Part A)

The 2019 breach was managed in a more reactive way, with a response focused on the acute issue, the actions of the member of staff who had inappropriately access patient records, without organised review of the context and root causes. Policies existed but were not robust in terms of driving staff understanding regarding confidentiality. Training was light-touch. System controls were limited by IT. Opportunities for structured incident analysis, early apology, and transparent engagement were missed.

The 2022 breach demonstrated a markedly improved organisational response: with rapid escalation, a comprehensive audit, immediate HR and police involvement, and proactive notification of almost 300 affected patients. However, communication gaps and limited follow-up persisted.

Across both breaches, systemic weaknesses such as legacy IT and electronic record systems, broad role-based access permissions, limited audit capability, unclear governance roles, and insufficient practical guidance, were as important as individual misconduct. The review found no evidence of intentional concealment by KEMH or FIG but identified a lack of structured learning.

Assessment of current information governance (Part B)

Since 2019, KEMH and FIG have strengthened policies, training, access controls, and audit processes. Staff awareness has increased, and managers recognise the importance of confidentiality. However, the current system remains fragile and heavily dependent on individual effort. Legacy electronic patient record infrastructure continues to pose the single greatest unresolved risk. Cultural anxiety persists among staff, and public trust remains significantly eroded, with survey results showing divided confidence in how information is handled.

Policies broadly align with NHS best practice principles, including the Caldicott Principles, but are inconsistently implemented, and not yet supported by a coherent, integrated governance framework. The Caldicott Guardian role lacks clarity, visibility, and defined authority.

Environmental risks such as overheard conversations, shared computer terminals and visible paper notes, continue to undermine confidentiality and trust.

Overall conclusions

The organisation has made meaningful progress, particularly since 2022, but information governance is not yet mature, consistent, or fully assured. Improvements have been incremental rather than strategic. To rebuild trust, KEMH and FIG must adopt a more integrated, transparent, and patient-centred approach, supported by modern systems, clearer leadership roles for information governance, and practical guidance for staff.

Recommendations

In undertaking this review, we were asked to make recommendations for implementation. The following actions represent what we judge to be the most immediate priorities: practical, tangible steps that can reasonably be taken to strengthen privacy and confidentiality arrangements within the Health and Social Services Directorate.

These recommendations are not exhaustive. Maintaining an appropriate balance between privacy and the sharing of clinical information in the patient's best interests requires continual wise judgement. Information governance is inherently complex; organisations must adapt to new legislation and technology, new risks, and threats, evolving guidance, and learning from experience as part of a continuous improvement cycle. These recommendations are intended to facilitate that continuous improvement journey.

It is also important to acknowledge that no organisation can guarantee the prevention of all future privacy breaches. Across the UK, incidents occur regularly, including within organisations that have strong and mature information governance systems which exceed the required standard.

However, by implementing these recommendations, the Health and Social Services Directorate is at a turning point. The focus is shifting from a narrative shaped by past breaches to forward-looking, with cross-organisational confidence that robust arrangements are in place to manage confidential data effectively and minimise risks to patient privacy.

Strategic leadership and framework

1. DHSS should develop an action plan to implement these recommendations. The draft action plan should be consulted on, seeking feedback from staff and patients, including patients with lived experience, prior to approval at the Health and Medical Services Committee (HMSC).
2. In completing the action plan arising from this report, and other inspections, DHSS should move to publishing regular self-assurance data regarding information governance metrics and assurance e.g. incidents, breaches, audits and controls, through the HMSC, in the form of an annual account. This should be accompanied by an annual continuous improvement plan and audit calendar.
3. DHSS should publish an overarching information governance framework that sets out the suite of information governance policy and guidance, defines clear roles, accountability and escalation routes, including defining the responsibilities of the Caldicott Guardian, Information Governance Lead, and senior management team.

Policy and process

4. DHSS should agree a clear, locally owned "*duty of candour*" policy. The policy should clarify the differences between organisational and professional duty of candour and reference the NHS *Saying Sorry* guidance or equivalent.
5. DHSS should review and strengthen its complaints policy to ensure clear entry points, consistent leadership of complex cases with a single point of contact for these, a defined approach when resolution is difficult, and an emphasis on early apology and resolution.

Caldicott and confidentiality leadership

6. DHSS should develop a network of Caldicott, or Confidentiality Champions, across all services and staff groups. Their role would include assisting the Caldicott function by supporting staff with confidentiality and information-sharing problem solving and transparency about information use in everyday practice.

Systems and technical controls

7. DHSS should replace or upgrade the current electronic patient record system (EPRS) to enable modern security, audit and functionality.
8. Within the current EPRS and with any new procurement DHSS should review the arrangements for the most sensitive confidential information in the electronic patient record to either:
 - i. Demonstrate that the need for clinical access in an emergency is greater than the need to reduce the risk of further confidentiality breaches; OR
 - ii. To introduce further safeguards in the EPRS such as introducing the confidentiality module and training staff how to use it appropriately.

AND justify the approach in line with all the Caldicott principles through a paper to the HMSC for approval of the rationale and consequent chosen approach.

9. DHSS should demonstrate reduction in environmental confidentiality risks that arise from the physical environment e.g. reducing corridor conversations, using a private space for confidential discussions, and removing paper and records from unattended desks and surfaces.

Training and culture

10. DHSS should develop concise, practical confidentiality and information-sharing guidance for staff.
11. DHSS should deliver both mandatory e-learning, and face-to-face discussion for all groups of staff. This should include case-based scenarios on legitimate access, duty to share, handling mistakes and business continuity plan tests. Training should include promoting a just culture and celebrating success; and encouraging self-reporting of errors without punitive response where appropriate⁵
12. DHSS should require all staff, including senior leaders, to discuss and agree their responsibilities for confidentiality in their next annual review and be able to evidence that all staff understand their responsibilities (Caldicott Principle 5) and are included in objectives where appropriate.

Patient and Public Involvement

13. DHSS should establish mechanisms of two-way open dialogue as consultation with all stakeholders about ongoing information management, information governance and proposed significant changes. This should include staff, and individual patients with lived experience