

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

Foreword

Welcoming independent insight and accountability

As Sponsor of this external review into our health service confidentiality arrangements, I welcome the publication of this report.

When the Falkland Islands Government (FIG) and the King Edward VII Memorial Hospital (KEMH) commissioned this external review, our goal was clear: to confront our past handling of data breaches with absolute honesty. We recognise that when confidential health information is held by an organisation, a fundamental duty of trust exists. Patients must have full confidence that their personal data is treated with the highest standard of care and respect.

This report provides an essential, objective baseline that allows us to look closely at our current arrangements and where improvements can be made. I want to express my gratitude to the experienced review team for their rigorous work. I also want to thank the members of the public, particularly the Justice4Patients group, who worked with us to shape the terms of reference. Their persistence ensured that this process captures the true impact of these events on our community.

A commitment to privacy and continuous improvement

Protecting patient privacy is not a static task, but a continuous journey of quality improvement. We accept the findings of this report in full and are using its recommendations as a powerful turning point to elevate our institutional standards and restore public confidence.

True quality improvement requires complete openness, which is why we are taking immediate action:

- **Unredacted Transparency:** This report is published openly and without redactions to ensure full public visibility.
- **Concrete Action Plan:** KEMH will deliver a local, practical action plan within the next six months to turn these recommendations into reality.
- **Public Progress Tracking:** Implementation will be actively monitored in the open sections of the Health and Medical Services Committee.

We cannot alter the past, but we can shape a safer future. We are entirely committed to building a more resilient, transparent, and high-quality health and social care service that our community can rely on.

Andrea Clausen

Project Sponsor

Chief Executive Falkland Islands Government.

Review team:

- Dr SJ Louise Smith – Registered Doctor, Consultant Public Health, Caldicott Guardian, Deputy Director Clinical Governance, UK Health Security Agency
- Mrs. Helen Dyer – Registered Nurse, Vice Chair UK Caldicott Guardian Council, Clinical Director Checked Ltd
- Ms Lara Kontos – Workforce Development Lead (UK Overseas Territories), UK Health Security Agency

Acknowledgements

The review team thank the staff of KEMH, the Directorate of Health and Social Services, the Falkland Islands Government, Justice4Patients (J4P), and service users for their transparency, cooperation, and assistance during the conduct of this review. We particularly acknowledge the Director of Health and Social Care who ensured that we were able to gather the information we needed for the review.

Importantly, we recognise that this review was made possible by the tireless campaign of J4P. Their advocacy has been central in driving this review and in pressing for continuous improvements in confidentiality.

We also thank staff and members of the public who took part in interviews, focus groups and surveys, and who engaged with the review openly and constructively. Their willingness to share their experiences, and insights, was vital to understanding both the historical events under review and the current information governance arrangements. We recognise that participation was uncomfortable for some contributors and we value the courage shown by staff and patients, especially J4P members, directly affected by the data breaches.

We are grateful for the Falkland Islands' radio, television, and newspaper media teams' support to their audiences and for spreading the word about the opportunity for everyone to participate in the review. We also thank those who supported the review through the provision of documentation, coordination of meetings, and practical assistance during the review team's visit. We are grateful to the Malvina House Hotel for providing a neutral environment to meet with stakeholders.

We recognise the contribution made by all stakeholders in facilitating an independent and comprehensive review. Their cooperation reflects a personal commitment to learning and improvement. Throughout this review we have recognised and applauded the willingness of all at KEMH to fulfil the obligations listed in the review's Terms of Reference.

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 appropriate.
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.

Table of Contents

Foreword.....	2
Review team.....	3
Acknowledgements.....	3
Executive summary.....	4
Recommendations.....	6
Table of Contents	8
Background and context	10
Health and Social Care in the Falkland Islands	10
Directorate of Health and Social Services (DHSS).....	10
Directorate of Health and Social Services Strategy	10
Information governance in context	11
Overview of the 2019 and 2022 data breaches	11
Terms of reference, aims, and scope of the review	12
How the review was conducted	13
Review initiation	13
Document collation and communication.....	13
Initial analysis.....	13
Review team visit.....	14
Analysis, validation, and report drafting	14
Part A – Look back.....	15
Applicable legal and policy frameworks.....	15
UK legislation and NHS policy context	15
Falkland Islands legislation and health policies	16
Timeline of the data breaches.....	16
The 2019 Breach	16
KEMH response to the 2019 breach.....	16
The complaint relating to the 2019 breach	17
The 2022 breach.....	18
Constitutional claim.....	19
Lessons learned by the health service.....	19
Key findings from look back.....	21
Introduction	21
1. Circumstances of the data breaches and contributory factors.....	21
2. Decision-making in handling the breaches	24

3. Processes, policy compliance; and 4. Missed opportunities.....	25
5. Improvements since the 2019 data breach	28
6. Engagement with those affected	31
Summary of part A: Learning from look back.....	34
Key conclusions.....	34
Thematic learning.....	34
Part B: Findings - current information governance & confidentiality	36
Introduction	36
CQC style inspection 2025	36
Current perspectives on information governance.....	37
1. Standards, compliance, and good practice	40
2. Policies and guidance on confidentiality.....	41
3. Openness, transparency, and apologies	42
4. Leadership and accountability for information governance.....	43
5. How patient information is stored and accessed	44
6. Staff training and organisational culture	44
7. Changes made since the data breaches	45
8. Audit, oversight, and ongoing assurance	45
Recommendations	49
Appendix A: Terms of reference	50
Appendix B: Public apology	55
Appendix C: Caldicott Principles.....	58
Appendix D: Documents reviewed.....	61
Appendix E: Information governance policy & practice analysis	68
Appendix F: Interviews & key lines of enquiry.....	74
Appendix G: Interview findings.....	78
Appendix H: Focus group findings	81
Appendix I: Public survey	84
Appendix J: Staff survey	90

Background and context

Health and Social Care in the Falkland Islands

The Falkland Islands are a British Overseas Territory with a population of around 3,700. Health and social care for the local population are provided by the Health and Social Services Directorate (DHSS), mainly through King Edward VII Memorial Hospital (KEMH). The service is a GP-led integrated service delivering emergency, primary, secondary and community care, alongside social care. Services are supported locally through arrangements such as telemedicine, visiting specialists, and for some, further care is provided outside of the islands.

In addition, a Medical Centre at Mount Pleasant Complex provides primary care to the Ministry of Defence and other eligible people. This service was outside of this review.

As KEMH is the only provider on the islands for residents, public trust in local health and care services is especially important. The Falkland Islands are a close-knit community with strong social ties and high levels of mutual support. Facebook, other social media platforms, and local media are important channels for communication.

Directorate of Health and Social Services (DHSS)

The Director of Health and Social Services leads the service and reports to the Chief Executive of the Falkland Islands Government (FIG) in their role as the head of public services.

The Chief Medical Officer, and Chief Nursing Officer, who report to the Director, in turn oversee clinical and professional standards and governance across medical services, nursing, and allied health services. Information governance leadership, including confidentiality and data protection arrangements, is from the Healthcare Governance Manager who is accountable to the Hospital Manager, overseen by the Director of Health and Social Services.

Oversight sits with the Legislative Assembly of the Falkland Islands, a unicameral legislature established under the 2008 Constitution and made up of eight elected Members, one of whom holds the portfolio for health and social services. The Health and Medical Services Committee provides political oversight and scrutiny of health and social care service policy and performance.

Directorate of Health and Social Services Strategy

The Directorate of Health and Social Services is currently developing its strategy to set its direction for the coming five years.

The draft strategy includes a specific goal to ensure robust health and social care information systems are in place. Upgrading these systems, strengthening information governance and confidentiality practices are recognised priorities. These commitments are supported by draft objectives and performance indicators including confidentiality training for staff, signed confidentiality agreements, and ongoing audits of data-handling practices. Prioritising information governance in the health and social care service's strategy would be an important contribution to strengthening privacy and confidentiality for service users.

A UK Care Quality Commission (CQC)-style inspection of some KEMH hospital services (but not social and community care services) was carried out in January 2025. It provides important

context and serves as a key reference point for this review. This report draws on its findings where relevant.

Information governance in context

Information governance carries sensitivity on the Falkland Islands. Local people have limited alternatives to the Directorate of Health and Social Care as their provider. Confidence that personal and medical information is managed safely is therefore critical to those seeking services.

FIG and DHSS are major local employers. Staff are also patients. Personal, professional, and community relationships often overlap, which can blur communication boundaries, especially when people use informal ways of communicating. This closeness makes privacy and confidentiality more sensitive and increases the chances and consequences of things going wrong.

As in all health systems, information governance has become more complex over recent years. The move to electronic patient records, the growing amount of data held, increased public awareness of data rights, and wider use of digital technology increase both expectations and risk. Cyber security and system resilience are particularly challenging in remote settings which use older information technology infrastructure.

Overview of the 2019 and 2022 data breaches

In both data breaches, clinical support staff accessed electronic patient records without a clear clinical reason or legitimate direct care relationship with the patient. Although they were employees, the access was outside their service responsibilities. Neither employee was a regulated healthcare professional.

Both incidents resulted in criminal proceedings. The 2019 breach also led to a prolonged complaints process. Following the 2022 breach, a public campaign known as Justice4Patients (J4P) was established by one affected family and others affected by the incident. For ease of reading, this report uses the term Justice4Patients (J4P) to refer both to the family directly affected by the 2019 breach and to the group established after the 2022 breach.

The breaches and associated events prompted wider public concern about the security of electronic patient records, how the health service responded to breaches, and the transparency of FIG and KEMH in relation to confidentiality.

The issues led to a constitutional claim by J4P against FIG, which was ultimately resolved through a Supreme Court Consent order. This review and report are part of that order.

Terms of reference, aims, and scope of the review

The aims and scope of this review were in a published Terms of Reference [Appendix A] and include independent assessment of:

- *How the information governance data breaches in 2019 and 2022 were responded to by KEMH/FIG, including lessons learned; and*
- *The current arrangements in relation to information governance and patient confidentiality at KEMH.*

Additional ambitions were:

- *To provide a balanced overview to the public of the current arrangements in relation to information governance and confidentiality at the KEMH via the means of a public report.*
- *To provide the basis for an achievable local action plan to drive further improvements in relation to information governance and confidentiality in KEMH and more broadly across FIG.*
- *To promote openness and transparency in relation to information governance and confidentiality at the KEMH to promote public reassurance in these matters.*

Both FIG and J4P agreed the attributes required of members of the review team in the terms of reference. Each assured themselves of these, through appropriate due diligence, prior to the commencement of the review.

The terms of reference ask the review team to author an independent report to be published unredacted.

The outcomes extend beyond this report. KEMH will ensure that an action plan is drawn up. Its implementation will be monitored in the open section of the Health and Medical Services Committee and by setting out how they will address the review's recommendations.

How the review was conducted

This section summarises how the review was undertaken. Further detail is provided in the appendices referenced below.

The review focused on organisational systems, governance, and learning. It did not re-investigate individual conduct as this has already been subject to disciplinary, regulatory, and/or criminal processes.

Review initiation

The review started with agreement by the review team to the published Terms of Reference (Appendix A). A confidentiality and data-sharing agreement was signed to ensure secure handling of information and to support open engagement with stakeholders. Initial meetings were held with KEMH leadership and J4P to explore and explain the review process, confirm independence, and set expectations for engagement.

The review team used the detailed Terms of Reference to draft Key Lines of Enquiry (KLOE) which were shared with both J4P and KEMH. These gave a structure for all evidence-gathering and analysis and formed the basis for interviews and data gathering [Appendix K].

Document collation and communication

A detailed document request, receipt, and review process was established. A total of 232 documents were received from KEMH and FIG, of which 54 were duplicates. Documentary evidence was also invited and received from J4P, many of which duplicated those from KEMH and FIG. Documents reviewed included:

- Policies and procedures
- Audit logs and access records
- Investigation reports and complaint correspondence
- Job descriptions and organisational structures; and
- Risk management and governance documentation.

More detail is available at Appendix D – Documents Reviewed.

A communications and engagement approach was agreed at meetings with both parties to support transparency. Two anonymous online surveys were designed by the team, reviewed by KEMH and J4P and distributed to stakeholders:

- A public survey; and
- A staff survey.

Survey questions and summary results are set out in Appendices I and J.

Initial analysis

Semi-structured interview schedules were developed based on the Key Lines of Enquiry. These were tailored for different stakeholder groups, including governance leads, clinical staff, non-clinical staff, and service users. Interview details are provided in Appendix F.

Data-collection templates were prepared, and initial document analysis commenced prior to the visit.

Review team visit

Members of the review team joined the Falkland Islands between 26 January and 3 February 2026. During this period:

- 25 interviews were conducted, including senior leaders from DHSS and FIG, clinical and non-clinical staff, the Caldicott Guardian, patient representatives, and J4P. The findings from these interviews are in Appendix G.
- Six themed focus groups were offered, covering managers and senior staff, staff employed before and after 2022, nursing staff, affected members of the public, and the wider public. Findings are summarised in Appendix H.
- Meetings were held with J4P both collectively and individually.
- A site visit to KEMH was undertaken to understand records storage, physical access controls, and training delivery arrangements. A similarly focused visit was made to Tussac House.
- As part of public engagement, the review team also participated in media interviews with local radio, television, and print outlets.
- Reviewers explored a little of the geography, wildlife, and facilities of Falkland Islands.

After returning to the UK, the review team conducted further virtual interviews with former directors and received additional documentary evidence.

Analysis, validation, and report drafting

Evidence from documents, interviews, focus groups, and surveys was analysed and triangulated across sources. Local policies and practices were reviewed alongside relevant NHS guidance where relevant to the Falkland Islands context.

A chronology of breach detection, escalation, decision-making, notification, and organisational response was developed.

Draft findings were shared with KEMH and J4P with a request to check for factual accuracy prior to drawing conclusions and making recommendations. Final drafting and iteration followed, incorporating corrections where appropriate while maintaining the independence of the review.

Part A – Look back

This section examines how KEMH and the FIG responded to the data breaches identified in 2019 and 2022. It looks back at what happened, how decisions were made, how affected individuals were engaged, and how these responses aligned with relevant legal and policy frameworks at the time.

Applicable legal and policy frameworks

UK legislation and NHS policy context

In the UK, patient confidentiality and information governance are underpinned by a combination of statute, common law, regulation, and professional and organisational guidance. Key elements of relevance to this review include:

- The *Information Governance review* titled *Information: To Share or Not to Share?* (2013) by Dame F Caldicott, a framework for managing patient and service user information in healthcare, balancing confidentiality with appropriate information sharing to improve care, underpinned by the Caldicott principles and UK data protection law.
- The *Health and Social Care Act* 2008, 2012 and *Health and Care Act* 2022, which set out statutory powers and duties for the handling of health data.
- The *NHS Act* 2006, which sets out what NHS organisations can and cannot do and how they can or cannot use information.
- The *General Data Protection Regulation* (GDPR) and the *Data Protection Act* 2018, which came into force in May 2018 and, together with the common law duty of confidentiality, form the core legal framework for handling personal health information in the UK and the basis for regulatory guidance from the Information Commissioners Office.
- The *Review of Data Security, Consent and Opt-Outs* (2016) from the National Data Guardian for England which led to the adoption of three leadership obligations and ten data security standards. It formed the basis of a national mandatory self-assurance model, the *Data Security and Protection Toolkit*, undertaken by tens of thousands of organisations in the UK Health and Care sector each year.
- *National Data Guardian Guidance about the appointment of Caldicott Guardians, their role and responsibilities* (2021)

A more extensive list is available from the UK Caldicott Guardians Council: [Other key legislation — UKCGC](#)

GDPR establishes 7 key principles, including lawfulness and transparency, purpose limitation, data minimisation, accuracy, secure handling, and accountability. Since 2018, these principles have been supported by detailed national guidance clarifying organisational responsibilities and operational practice within the NHS in the UK which can be accessed here: [Information governance - NHS England Digital](#).

Falkland Islands legislation and health policies

UK GDPR and the *Data Protection Act 2018* do not extend to UK Overseas Territories, including the Falkland Islands. NHS rules and policies therefore have no legal force locally unless adopted through Falkland Islands legislation, policy, or contract.

The primary legal instrument for the management and use of personal and medical information in the Falkland Islands is provided by the Constitution, which establishes a right to private and family life. This includes protection against unlawful access to, or disclosure of, personal health information. These rights are legally enforceable.

The Falkland Islands also have the *Access to Health Records Ordinance 1995*. Legal advice provided by the Attorney General in February 2019 stated that this legislation grants patients the right to access their medical records but does not extend to a legal right to receive information about who has accessed those records (audit trail data). This differs from the broader SAR (Subject Access Records) rights available under GDPR in the UK.

The *Falkland Islands Crimes Ordinance 2014* provides a further statutory instrument which has been relevant in relation to previous data breaches, particularly *Part 14 – Computer Misuse*.

Caldicott Principles were explicitly incorporated into the *Health and Social Services Directorate's Code of Confidentiality* in August 2019

In 2020, FIG introduced a local *Data Protection Policy*. This policy reflects GDPR-style principles but is not legally identical to UK GDPR.

Timeline of the data breaches

The 2019 Breach

On 17 January 2019, the Chief Executive of FIG and the Attorney General agreed to an IT audit in a meeting with the family of a deceased patient whose care, in 2017 and before, was under investigation. The purpose of the IT audit was to identify which staff had accessed the patient's electronic clinical record, and the records of named family members.

This took place the following day on 18 January 2019. It showed four staff members who had accessed the records but appeared not to have a clear clinical, or supporting role, in the patient's care.

KEMH response to the 2019 breach

KEMH recognised that the identified access could have been inappropriate and needed more investigation. An initial investigation by KEMH in January 2019 led to further disciplinary investigation - undertaken by the incoming hospital manager and FIG Human Resources (HR). Actions taken included:

- Suspension of staff.
- Further audits of access to specific records.
- Assessment of whether staff could justify access to the records.
- Referral of two staff who could not evidence justification to formal HR disciplinary processes.

- A commitment to review information governance arrangements, policy, and procedure.
- A commitment to introduce additional classroom based training and written documents to ensure full understanding by staff.

At the conclusion of the investigation in April 2019, written communication and an apology was sent from the Director Health and Social Services to an affected patient and family member. The letter sent to the family states in the last paragraph: *"I recognise that a matter such as access to medical records can be of concern and I am sorry for any distress this process and our findings may have caused you."* Having had an unscheduled face-to-face meeting and followed this up with this letter, the Director stated that they did not perceive that a further face-to-face meeting with the family was necessary.

Additional audits were undertaken, including repeat reviews later in 2019, which further confirmed that while most access could be justified on clinical or administrative grounds, 4 staff appeared to have accessed records without authorisation. This includes the 2 referred above.

Ultimately, investigations concluded that 2 staff members had accessed the record but had not accessed detailed clinical information inappropriately. They were given written formal warnings. The other two were "dealt with through the disciplinary process." Disciplinary processes were completed in line with contemporaneous policy for these two individuals. One of these was suspended and later resigned during the investigation process. Disciplinary procedure for this employee ceased at the completion of their contract.

In August 2019, the family reported the matter to the Falkland Islands Police, who conducted their own investigation.

In July 2020, one individual was charged with multiple computer misuse offences under the *Crimes Ordinance*. In early 2021, the court case concluded with a not guilty verdict. The court found that although records had been accessed without authorisation, it had not been proven that the individual knew their access was unauthorised.

The complaint relating to the 2019 breach

A formal complaint about inappropriate staff access to confidential patient information was made to Directorate Health and Social Services in May 2019. At that time, the initial management audit and investigation had been completed, and disciplinary actions were underway. Findings had been shared with the family, through correspondence, but there was no further face-to-face meeting at this time. The family were not satisfied with the way that the breach had been responded to, nor communicated with them. They also thought that technological controls should have been put in place to prevent the breach.

Between December 2019 and July 2023, the complainants made regulatory referrals about senior KEMH health professionals to relevant professional bodies. By July 2023, the relevant professional bodies had concluded that no further action was warranted.

During this period, progress with the management of the complaint was affected by the COVID-19 pandemic lockdown from March 2020, and by a parallel police investigation leading to court proceedings in early 2021. The complaint was formally closed by KEMH in June 2021. An appeal made by J4P in August 2021 was considered and closed by the FIG Chief Executive in November 2021 after twice meeting with them (1st September and 15th October).

As part of FIG's response to the appeal, more remedies were agreed, including an IT professional independent of FIG to examine a set of medical records to ascertain if they had been inappropriately altered. A targeted patient record access review and audit was commissioned according to a terms of reference agreed with the family. This was completed in 2023 with additional technical support from FIG and consultation with EMIS, the medical record system provider. It covered the period from June 2017 to September 2023 and offered assurance that the family records had not been inappropriately altered and that further inappropriate records access had not been missed or concealed by KEMH activity.

There was a commitment within the response to the appeal that the Chief Executive would oversee an information governance review conducted by FIG at KEMH. The aims of the review were to *"achieve sustained learning and improvement through a positive forward-looking piece of work."* This review was undertaken by FIG.

The response also offered a financial remedy as compensation for *"Distress caused by the subject matter of the complaint, risk of reputational harm, time and trouble, personal outrage, time taken to respond to the complaint"* and included multiple apologies including that FIG had not followed its own policies and procedures. This offer of compensation was not accepted by J4P on the grounds that they did not believe that their questions had been fully answered nor that the underlying issues had been fully addressed.

J4P asked FIG to make the public aware of the breach. FIG did not accept this request, stating that there was no evidence that anyone else's records had been accessed and that issuing a public statement could raise concerns and undermine public confidence *"in an institution where that public confidence and trust is paramount particularly at a time when we continue to deal with the impacts of COVID19"*.

The 2022 breach

In October 2022, at the request of J4P, a further IT audit took place to identify which staff had accessed their family's clinical records between May and October 2022. The audit showed 4 staff names whose access to one record could not immediately be explained. Further investigation offered assurance that three of these were legitimate, but concerns remained about the fourth who had accessed the record once on 9th August 2022. The family were notified of this.

KEMH decided to do a further audit. This audit identified inappropriate access to further patient records by this member of staff working in community services. The staff member was immediately sent home and their access to medical records was blocked pending further investigation.

KEMH held a wider investigation to review this individual's access to electronic patient records across the system. By October 2022, following review of all patients registered on the electronic system (in effect the entire population), nearly 300 patient records were identified as having been accessed without a clear work-related reason.

The Director of Health and Social Care informed the FIG Chief Executive and the Attorney General. Falkland Island Police were notified, and internal HR disciplinary processes were initiated.

A structured approach was taken to notify all affected patients. Template letters were developed, staff were briefed, and liaison took place with mental health services to identify and support those considered most vulnerable. A decision was made that letters should, if necessary be delayed. This was to ensure affected patients received them at the beginning of a week when professional support would be available to them. On 5th December 2022, letters were sent to all identified patients informing them of the breach. Consideration was given as to who to advise for children under the age of 16. The letters contained detail of who to contact for further information or questions.

The letters prompted a substantial email response to KEMH from affected patients and other concerned individuals. A further 54 patients requested a specific audit of their records to identify who had accessed them.

In December 2022, KEMH briefed the MLA ahead of a Legislative Committee meeting. As the police investigation was ongoing, it was considered inappropriate to share detailed information publicly. However, assurance was provided that the breach involved a single staff member who had by then been dismissed, and that anyone who had not received a letter or phone call from KEMH had not been identified as affected. It was also confirmed that access rights had been reviewed again and remained appropriate to staff roles, given the limitations of the Electronic Patient Record System (EPR).

Following Police investigation, in March 2023 the former staff member was charged with computer misuse offences under *Crimes Ordinance*, pleaded guilty, and was sentenced in May 2023.

Constitutional claim

In July 2023, a request for an independent inquiry was made by J4P to the Governor of the Falkland Islands. This was considered. However, in November 2023 the Governor responded to advise that there were no grounds to proceed.

In December 2023, a “*letter before claim*” was issued via solicitors by J4P to the Chief Executive of FIG. The letter asserted that the unauthorised access to medical records had been a breach of the protection for private and family life under Section 9 of the *Falkland Island Constitution*.

A settlement was agreed through a Supreme Court order in October 2025. This comprised a public apology for unauthorised access to medical records to be made by FIG in the Legislative assembly in August 2025 (Appendix B), and an independent review (this review) to be commissioned.

The *Supreme Court of the Falkland Islands Order* stated that the Director of Health and Social Services and the Governor of the Falkland Islands [the respondents] had breached the constitutional right to respect for privacy and family life of the 5 individuals [plaintiffs] and should pay financial compensation to them and pay the reasonable costs of the claim. The consent order did not address compensation for other affected individuals who were not named in the action.

Lessons learned by the health service

By August 2023, multiple policies relating to records management, record keeping and information governance had been reviewed and republished by KEMH. In the same month, the

Senior Management team at KEMH conducted a “*Lessons Learned*” review from both breaches and created an action plan for further development.

The Director Health and Social Services issued a detailed press statement updating the media, and public on the detailed list of actions that had been taken by the Directorate. The changes that had been implemented by September 2024 included:

- Reviewed individual user profiles to ensure staff only have the minimum access needed for their role.
- Electronic patient data accessible only on KEMH-owned devices with individual, non-shared logins.
- Formal, auditable process for managers to request access for new staff.
- User accounts disabled promptly when staff leave.
- Collaboration with FIG Records & National Archives to review practices, develop policies, audit data handling, and improve physical security of paper records.
- Regular bi-monthly spot checks on electronic record access using defined criteria for identifying potential unauthorised access.
- Updated confidentiality policy including a clear process for managing suspected data breaches.
- All staff (including new starters) have signed the updated confidentiality agreement.
- Confidentiality training delivered at induction and refreshed at least every two years.
- Mandatory information-governance training for all staff.

By the time of this review no further complaints related to patient confidentiality had been made to KEMH to end 2025. This contributes to the review team’s conclusion that information governance management is improving.

Key findings from look back

Introduction

This section reviews the two data breaches. It is structured to directly address the specific questions set out in the Terms of Reference and focuses on organisational response, decision-making, and learning.

Terms of Reference

- Specifically, to critically review the approach to detecting, assessing, managing and reporting data breaches in relation to previous data breaches, and in addition to review;
 1. The circumstances in which previous data breaches occurred and identify contributing or causative factors to these breaches.
 2. The decision-making in relation to the handling of previous data breaches, and requests for audit trails within the KEMH and in the FIG corporate decision-making structure (including decision making about referral to the Police).
 3. The processes followed in respect of each previous data breach, and whether these complied with policies which were extant at the time or relevant deemed best practice in the NHS, including the duty of candour.
 4. Identifying any missed opportunities which would have improved the quality of the response in each instance and aligned the response with recognised best practice.
 5. Understand improvements made after the 2019 data breach and identify further learning opportunities with respect to previous data breaches, including those already acted upon by the KEMH, and those which would further strengthen information governance for the future; and
 6. Review the approach taken by KEMH and FIG in relation to engagement with those affected by the data breaches to identify any lessons learned or missed opportunities, particularly in relation to whether NHS best practice was followed for appropriate apologies, keeping those affected victims updated and offering support.

1. Circumstances of the data breaches and contributory factors

“The circumstances in which previous data breaches occurred and identify contributing or causative factors to these breaches.”

Context at the time

Reviewers explored but found no historic local cases which established precedent in relation to breach of the common-law duty of confidentiality in the Falkland Islands. Nevertheless, despite the absence of local legal precedent, public expectation that such a duty exists is undisputed. In addition, a universally accepted professional duty of confidentiality in relation to medical care has been in place since Hippocrates and is widely accepted as essential for health care. It is therefore accepted that in both breaches, a duty of confidentiality was owed to patients. The

most common way for the duty of confidentiality to be satisfied is that the patient consents to their medical record being accessed by an individual staff member for the purpose of direct care and local audit, this consent is usually assumed to have been given through the request for medical care.

Both breaches involved unregistered clinical-support staff who had been deemed to require clinical level access to carry out the clinical support functions of their roles. This meant that there would be times when they would need to access any part of the record for patients on their department's caseload. The role-based access set-up in the electronic record meant that their access was to clinical records in all departments.

The access they made to specific named patient records in these data breaches were considered inappropriate because their reason for access could not be justified to be part of the patient's care journey. They were not opening the record to undertake legitimate clinical support actions.

The response to the 2019 breach over the following years took place in a challenging environment and can be seen to have been influenced by:

- The leadership and delivery of the COVID-19 pandemic response from March 2020.
- Changes in senior personnel leading the response to the data breach – specifically the Health Service Director and Hospital Manager, and Falkland Islands Government Chief Executive.
- A small-community context in which the affected patients had been employees, part of the governing bodies and were known to staff, contributing to anxiety and caution in handling correspondence.
- Investigations related to the care of patients with mental health conditions.
- A unique model of integrated health and care service delivery in the Falkland Islands which requires input from visiting specialities, telemedicine, and external support from multiple countries.
- The electronic patient record system, although customised in some ways for local needs, was fundamentally an off the shelf system developed for use in UK primary care. In Falkland Islands it is used for primary, secondary and community care across all departments.

The review team considered contributing factors using a people, process, and technology framework. This analysis reflects the position at the time of the 2019 breach.

People – recruitment, induction and training, awareness, responsibility, and accountability

- Confidentiality training was in place in 2019 and was included in staff induction, but it is unclear how well staff understood how to apply confidentiality in their day-to-day roles.
- There is no evidence that staff did annual data security training appropriate to their roles, and learning needs, nor that they were asked to pass a mandatory test to demonstrate understanding.
- Confidentiality agreements were required, but evidence suggests that record-keeping and assurance were less rigorous than current practice.
- We have not seen evidence of an information governance framework being used as an effective overarching control and used at strategic decision-making level. We have provided a detailed policy analysis to inform a framework in Appendix E.

- Prior to 2019 there is evidence of a disbanded Information Governance Committee.
- Reminders were issued to all staff about confidentiality but expectations about consequences for inappropriate access were not explicit. The consequences of self-reporting an incident were unclear.
- The court found that in the 2022 breach there is evidence that the member of staff accessed records during working hours to alleviate boredom and curiosity. Malevolence was not shown by the review to be contributory.
- Job descriptions did not specifically refer to accountabilities and responsibilities for information governance lead roles e.g. strategy and development planning.
- There is no evidence to suggest that every employee's job description included reference to their individual responsibility to information governance within the organisation.

Process – access management and audit

- The review team did not see evidence of a robust process to assign appropriate levels of role-based access prior to 2019. Anecdotally this was at the discretion of the line manager and yet there were instances where other managers made decisions and line manager involvement was not consistent.
- There are anecdotal reports of shared passwords and log-ons.
- The review team found no evidence of a universally implemented clear desk policy.
- In 2019, there is little available evidence to suggest that any incident reporting and significant event analysis processes were in place for information governance events.
- The review team also found no evidence of timely near miss reporting or systematic reviews of processes which have caused such events.
- Consequently, there is no evidence of trend analysis for incident and near miss reporting to support a culture of self-reporting.
- The review team saw no evidence of a regularly tested continuity plan to respond to data security threats (UK standard is annual). Anecdotal evidence suggests that paper systems could be reinstated.
- A routine programme of access audits to identify unusual patterns of record access by staff or red flag occurrences was not evident at the time of the first breach.

Technology – systems and infrastructure

- DHSS relied on unsupported operating systems and legacy server-based electronic patient record software.
- These systems had limited access controls: making role-based access less useful as a control mechanism. There is facility within the EPR system for unique user accounts, session time-outs, and audit logs. However, access controls could not be limited to a defined patient case load.
- The patient record system in use can allow staff entering data to mark it as confidential, (referred to as the confidentiality module). Historically a decision has been made not to use this on the grounds of clinical safety. In a previous emergency staff had not known how to override the confidentiality protection and access the information.
- As an alternative approach, limited data masking was put in place for records holding particularly sensitive information. This comprised documents being attached rather than the data inserted directly. The attached documents require an additional step to open them, but are not password protected.

- There are no extra checks in place when someone tries to access these attachments that they would not usually access. Common examples of such checks include a pop-up asking the user to enter a reason for access or to 'break the glass', or asking if they are sure they want to open the file.

It is important to note that this review did not include a cyber-security or technical penetration assessment. It makes no findings regarding the presence of a cybersecurity strategy, contractual responsibilities of IT suppliers for protecting the personal confidential data that they process, or infrastructure security beyond documented system limitations. The reviewers did not see evidence of multi-factor authentication.

2. Decision-making in handling the breaches

"The decision-making in relation to the handling of previous data breaches, and requests for audit trails within the KEMH and in the FIG corporate decision-making structure (including decision making about referral to the Police)."

Decision-making in 2019

The first breach was identified when the family asked the Attorney General to undertake an audit of their records as part of an unrelated investigation in response to an earlier complaint. The issue identified by the audit was not initially recognised as a separate information governance incident and was therefore managed through a decision related to satisfying the (previous) complaint processes and not through any formal information governance breach investigation mechanism.

As a result, the early involvement of FIG, through the Attorney General (who was handling the previous complaint) meant that:

- Investigations were undertaken quickly but without an agreed, coordinated plan.
- Senior KEMH leaders did not formally agree a scope or desired outcomes for the investigation at the outset.
- Communication with the family evolved through multiple senior figures.
- NHS guidance about *Saying Sorry* (2018) did not appear to have been referred to.

Decisions were made by individual executives acting in good faith and with appropriate concern about potential misconduct of a specific employee. For example, there is evidence that individual members of the senior management team issued written apologies before the formal complaint about the handling of the incident was made in May 2019. However, the absence of a coordinated incident response limited the opportunities for collective decision-making, structured learning, and clear communication.

The review found no evidence of any decision or action, formal or informal, to indicate that the seriousness of the issue was intentionally minimised or concealed. There is evidence that senior management team members viewed a breach of confidentiality as an unacceptable and serious incident.

The incident continued to be investigated, and ongoing decisions were made in response to the formal complaint of May 2019 and subsequent complaint correspondence. The review team have, at times, been unable to differentiate between the response and management of the data breach incidents, including organisational learning, and the handling of the complaint.

Referral to the police

The review has seen no evidence that KEMH considered reporting the 2019 incident to the police. In 2019, the Attorney General advised the family that they could report the matter to the police. He recused himself from making such a referral because he would be likely to be involved in any future action and wished to avoid a conflict of interest. At that stage, in the absence of established data protection law and case law, it was not clear to health service leaders that the behaviour of the member of KEMH required reporting to the police.

Audit disclosure

Requests from the family for the names of staff who had accessed records were refused by KEMH. This decision was consistent with local legal advice and reflected contemporaneous concerns about fairness, confidentiality, and the risk of identifying staff where allegations had not been proven.

Decisions about how audits were undertaken were technically complex and although efforts were made to explain these to the family, the repeated iterations may have contributed to ongoing dissatisfaction.

Decision-making in 2022

By contrast, decision-making in 2022 was quicker and more structured. Once inappropriate access was identified, and before the affected patients were advised by letter:

- A comprehensive audit was undertaken to identify all affected records.
- Senior managers and clinicians were briefed.
- Human resources were advised and took immediate action.
- Police referral was initiated promptly.
- Communication with different stakeholders was considered and a formal notification process was established.

This response demonstrated clear organisational learning from 2019: particularly the best practice of providing wellbeing support for vulnerable patients.

Inevitably, with large numbers of patients involved (nearly 300), it is possible that some individuals would not receive the information that their notes had been accessed inappropriately at the time, for example if the patient had changed address without notifying KEMH. KEMH did not use any method to enable them to record who had received notification.

3. Processes, policy compliance; and 4. Missed opportunities

This section reviews questions 3 and 4 in the Terms of Reference together as a single analysis to consider:

“The processes followed in respect of each previous data breach, and whether these complied with policies which were extant at the time or relevant deemed best practice in the NHS, including the duty of candour.

Identifying any missed opportunities which would have improved the quality of the response in each instance and aligned the response with recognised best practice.”

Information governance and GDPR principles

As part of this review, it has not been possible to fully establish which versions of specific information governance policies were in force at each point in the timeline. Current policies are listed in this report, and a review of key policy areas provides insight into how responses aligned with good practice is available in Appendix D.

Although GDPR did not apply locally in 2019, KEMH's actions i.e. acknowledging the breach, disciplining staff, notifying patients, and strengthening training, were broadly consistent with the spirit of both GDPR principles and the Caldicott principles.

In responding to the data breaches, KEMH initially declined to release information showing which staff had accessed the relevant patient records. This position was based on legal advice at the time from the Attorney General, which interpreted the Falkland Islands Health Ordinance as conferring a right only to access one's clinical records, and not to any associated audit-trail data such as staff access logs. This contrasts with UK subject-access legislation, where audit information linked to a record is within scope.

KEMH subsequently reviewed its approach and introduced local guidance enabling patients to request targeted audits of access to their own records, including the names of staff who viewed them. Although resource-intensive, this change reflects best practice for organisations seeking to demonstrate transparency and trustworthiness.

Complaints handling

The FIG complaints policy was followed procedurally with respect to the formal complaint in May 2019. Responses were issued, escalation was offered, and an appeal was considered by the Chief Executive.

However, the complaint process became prolonged and increasingly detailed in all parties' attempts to clarify proffered explanations. Efforts to centralise communication through a lead member of staff were very reasonable but appear to have been perceived by the complainants as avoidance. Each time a response was provided, it led to further questions or request for further details by J4P.

The process was ultimately closed by the Director of Health and Social Services without a shared understanding of outcomes. The Director thought that they had answered every aspect of the complaint to a reasonable standard. The closure of the complaint was not accepted by J4P, because they were not satisfied by the answers they had been given, exacerbated by their low levels of trust.

Organisational and Professional Duty of candour

The NHS statutory duty of candour does not, and did not, apply in the Falkland Islands. Even if it had, it is not clear that either breach would have met the duty of candour threshold, which is of a notifiable safety incident i.e. one which in the reasonable opinion of a health care professional appears to have resulted in severe harm, moderate harm or prolonged psychological harm to the service user.

Whilst the statutory duty of candour does not apply, regulated clinicians are subject to a professional duty of candour. The General Medical Council (GMC) and Nursing and Midwifery Council (NMC) have issued joint guidance since 2015: [openness-and-honesty-when-things-go-](#)

[wrong-the-professional-duty-of-candour-1224-2015.pdf](#). Our review found that several elements of professional candour were demonstrated including explanations of what had occurred, apologies, and written follow-up. However, these were not delivered through a structured duty of candour process. The absence of a formal incident review limited opportunities to define the scope of the incident and to explain learning and next steps to everyone involved but has not been found to have limited professionals' transparency.

In the NHS, the duty of candour is generally interpreted as requiring organisations to inform patients or their representative when something has gone wrong with their care. Organisations will also typically consider whether an incident poses wider population-level risk and whether public or media communication is required.

In the 2019 breach there is evidence that the potential for unwarranted public anxiety was considered. In 2022, although no public statement was made, a communication plan for all staff and affected individuals was developed and implemented.

The review team considers that Caldicott Principle 8 (established 2020), which relates to transparency in the lawful, ethical, and appropriate use of health and care information, was already culturally, although not systematically, embedded in KEMH in 2019. No evidence was found of intentional secrecy or obstructiveness. Instead, a clear wish to be open, kind and achieve resolution in this novel scenario was evident from all parties.

Finally, while clinicians have an individual professional duty to be candid with patients about their clinical care, organisational responsibility for information governance and privacy in the UK sits with the Information Commissioner. These regulatory requirements apply to organisations rather than individual practitioners.

Regulatory concerns and learning culture

Professional regulators reviewed referrals from J4P, who raised regulatory concerns about senior clinicians alleging a lack of candour, communication and leadership, inadequate training, monitoring, supervision and support of staff, and of granting access to electronic medical records for a member of staff who was unqualified and untrained. The regulators reviewed the referrals in detail and concluded that no investigations or actions were required. This review found no evidence to suggest any breach of professional duty requiring re-referral.

However, professional duty also includes promoting organisational learning following adverse events. The review found limited evidence of senior clinicians' involvement as leaders, and no clinical review following the 2019 breach. In contrast, a post incident review meeting, led by the Director of Health and Social Services, following the 2022 breach was held and included senior clinicians. This suggests that the missed opportunity from 2019 has already been recognised.

The role of the Caldicott Guardian at KEMH at the time of the 2019 breach was not clearly described. The role is usually advisory and offers guidance to the organisation to support decisions relating to the lawful ethical and appropriate use of confidential information. The Guardian is often a clinician because there is a need for them to understand the clinical use of data in the context of the clinical teams' practices and the patient pathway to be able to offer wise advice.

For example, it is good practice that the Caldicott Guardian in KEMH advised the decision-making process to enable, or disable, the confidentiality module, offering a patient safety-based rationale. Although this process, and the justification of the decision based on the Caldicott Principles could be more clearly communicated.

Significant event analysis

A significant event analysis (SEA) or formal root cause analysis (RCA) was not undertaken following either breach. There is no evidence to suggest that the events of 2019 were recognised as a serious untoward incident or significant event which might have triggered such an analysis. This represents a missed opportunity to identify system-wide issues, communicate learning, and move the focus away from individual conduct to organisational system-level response.

The “*Lessons learned*” meeting held in August 2023 was attended by the Director of Health and Social Services, the Hospital Manager, the Chief Nursing Officer and the Chief Medical Officer. Its purpose was to “*go through both sentencing report/court cases for the two ex DHSS staff members in 2021 & 2023 respectively to consider and act on any actions/DHSS weakness (specially for non-clinical staff) provided in the report.*” Actions were assigned to individual leads.

Following this, in July 2024 a detailed press statement to share the outcomes from this meeting was released. This process is identified by the review team as conscientious good practice.

5. Improvements since the 2019 data breach

“Understand improvements made after the 2019 data breach and identify further learning opportunities with respect to previous data breaches, including those already acted upon by the KEMH, and those which would further strengthen information governance for the future.”

Information governance improvements

Since the 2019 data breach, KEMH and FIG have implemented ongoing improvements in information governance. This has included regular updating of policies and guidance, the introduction of new training requirements, and the establishment of assurance activities such as routine electronic patient records access audits and a FIG *Data Protection Assessment* audit.

While improvements are evident across multiple areas, the review did not identify evidence of a single, time-bound, strategic plan for information governance development. Instead, progress has been achieved through incremental and ongoing development activity. Beyond the immediate actions taken following the 2022 breach, improvements appear to reflect continued organisational learning rather than a discrete post-incident reset.

People: Recruitment, induction, and training

Prior to January 2019, the health service had a code of confidentiality in place. There is evidence of periodic reminders to staff, including whole-organisation communications about confidentiality responsibilities.

Since 2019, recruitment, induction, and training arrangements have been strengthened. Changes include:

- Explicit questions on confidentiality at recruitment.
- Clearer coverage of information governance within induction.
- Mandatory information governance and confidentiality training for all staff.

- Confidentiality online e-training introduced.
- Monitoring of compliance with two-yearly refresher training.
- The introduction of face-to-face training for non-clinical staff.
- Consistent recording of individual induction and mandatory training completion.

These changes represent a material improvement in both consistency and assurance.

Process: Access management, review, and audit

Processes for managing role-based access to electronic patient records have been formalised. Access decisions now require sign-off by line managers who understand the operational detail of each role, supported by documented access criteria.

A routine audit programme has been established since 2021, reviewed and improved in 2023 and is now conducted quarterly on a random sample of staff. Audits check:

- Completion of mandatory training.
- Signed confidentiality agreements; and
- Whether staff are accessing their own or family members' records.

Additional developments include clearer guidance for patients who wish to request an audit of access to their own records, despite this not being a legal requirement locally.

In 2023 a *Data Protection Assessment* audit report and recommendation tracker was created by FIG for internal assurance. The aim of the assessment was to assess compliance around data protection. A series of actions were identified and were being tracked. Our review has identified this as good practice which should continue.

Also, in August 2023, a further patient record access review, was commissioned as an independent audit by FIG. This was done at J4P's request following consultation with the provider of the electronic patient record, EMIS. Its aim was to bring about a conclusion to the concerns raised by the complainants.

A term of reference for this targeted review was written by the Director of Health and Social Services and agreed with stakeholders. The terms of reference described the actions to be taken by FIG on receipt of the results. The actions included providing the full results to the complainants and notifying the police of any result indicative of criminal offences. The audit was completed and found no new issues or concerns. The results were accepted by J4P.

IT systems

Efforts have been made to improve the electronic patient record. However, progress has been constrained by reliance on legacy, server-based systems. Extensive procurement activity was undertaken in 2023, but technical limitations restricted what could be procured. Procurement of a new system is a priority for the directorate and renewed efforts to source a new EPR system were ongoing at the time of this review.

The IT infrastructure, and the Electronic Patient Record system, remain the most significant unresolved risks to information governance. This risk is recognised within the DHSS risk register, at the highest possible level of risk. The review team were advised of a basic business continuity plan which mentions this issue and anecdotally paper systems can be quickly established.

Policies and guidance

There has been a sustained series of policy development and reviews since 2019, covering information governance, confidentiality, complaints, incident reporting, records management, training, and acceptable use of IT systems:

- July 2019 - DHSS Information Governance - detailed policy and guidance V2
- July 2019 - Code of Confidentiality Policy amended to include Caldicott Principles and MCA
- October 2019 - Recruitment Selection Policy/ procedure.
- December 2020 - FIG Data Protection Policy V1 5.3.2 establishes a right of access to "personal data held by FIG".
- April 2021 - FIG DHSS Staff Induction Policy reviewed- V3 includes FIG induction checklist. (Confidentiality agreement signature required)
- August 2021 - Recruitment and Induction Policy/Procedures reviewed.
- September 2021 - Serious Event Analysis Standard Operating Procedure (SOP).
- November 2021 - FIG DHSS Incident Reporting Policy V1.
- April 2022 - FIG acceptable use policy ICT Version 1 replaces 2015 policy.
- July 2022 - Code of Confidentiality policy revised for new Caldicott Principles
- August 2022 - Recruitment and Induction policy/procedure reviewed - minor word change.
- December 2022 - DHSS Complaints Policy updated to include Q pulse & FIG corporate policy - for inclusion on website.
- February 2023 - DHSS Guidance re access audits of EPR V.1 published.
- August 2023 - DHSS Document Records Management Operational policy V2 published.
- December 2023 - Mandatory Training Policy V1 introduced; and FIG acceptable use policy ICT Version 1.1 "updated language".
- April 2024 - Criteria to Evaluate User Access in EPR established. Audit quarterly sample staff.
- July 2024 - Code of Confidentiality Policy revised and incident procedure added.
- August 2024 - DHSS Complaints Policy updated - to include head of care services.
- October 2024 - Access checklist (EMIS/security/Q Pulse) launched.
- February 2025 - Current Code of Confidentiality form introduced.
- Feb 2025 - DHSS Guidance Access Audits of EPR V1.1 Feb 25: process refinements made.
- March 2025 - Code of Confidentiality Policy revised and updated to include the revised Caldicott Principles
- March 2025 - DHSS Complaints Policy amended to include Caldicott role and responsibilities.
- April 2025 - FIG Whistle Blowing Policy V1.
- April 2025 - FIG Complaints, compliments, comments policy V1.8 published.
- Sept 2025 - Record retention schedule launched.

These updates demonstrate improved clarity, and alignment with good practice, ongoing review, and organisational learning.

While the volume and frequency of policy updates indicate commitment, they also reinforce the need for a strong governance framework, aligned with clinical governance, to ensure policies

are understood, implemented consistently, and translated into day-to-day practice to maintain patient safety.

6. Engagement with those affected

“Review the approach taken by the KEMH and FIG in relation to engagement with those affected by the data breaches to identify any lessons learned or missed opportunities, particularly in relation to whether NHS best practice was followed for appropriate apologies, keeping those affected victims updated and offering support.”

Expectations

The expectations of those who were owed a duty of confidentiality in relation to the 2019 breach were that engagement would reflect NHS duty of candour principles. They expected:

- Face-to-face communication
- A clear apology
- Updates on actions being taken in response to the breach; and
- Openness and transparency throughout the process

While these expectations are not surprising, the organisational duty of candour was not a legal or policy requirement in the Falkland Islands at the time and had not been formally adopted. It is also not clear that the 2019 breach met the definition of a notifiable safety incident that would trigger the use of the NHS duty of candour.

This may have created an unrecognised difference in understanding about what standard of engagement should apply in practice. No gap was found in professional practice in relation to the duty of candour.

Discussions with all parties suggest that expectations were shaped by past experiences. The review team considers that J4Ps perceptions – both of their own experiences, and those of others affected by the breach – along with their understanding of systems, processes, and standards, strongly influenced what they expected from the organisation’s response in both nature and scale. This sensitive issue was not directly addressed in communications.

There was a broader expectation that FIG would provide reassurance. People particularly wanted clarity about exactly what inappropriate access had occurred and why. However, when this level of detail was provided during the 2022 breach, it appears to have been interpreted by some as reinforcing a perception that FIG was trying to minimise the seriousness of the incident—for example, when the motivation was described as “*nosiness*” rather than something more malicious.

There was also an expectation of ongoing communication regarding system improvement and follow up which was made but only where specifically requested. The Directorate of Health and Social Services did not offer it proactively.

This review found that an unmet expectation of openness and transparency from patients and the public continues as a theme.

Face-to-Face engagement

Initially, discussion of the 2019 breach took place as part of an earlier, related complaint that had been escalated to the Attorney General, who took an early role in communicating with the family. Communication included telephone contact and some face-to-face discussions.

Health service executives met the family informally on an ad-hoc basis, including through unplanned encounters initiated by the family. Whilst during these contacts staff showed a willingness to engage and attempt to meet the family's demands, they were not part of a structured, planned or co-ordinated approach. By August 2021, requests from the family for further meetings were declined by KEMH on the grounds that all information had been shared in writing and there could be no further benefit.

In the 2022 breach, initial communications with those affected were proactively planned but follow up communications were not. There is no evidence of a planned organisational approach to handling responses. Instead replies were bespoke, managed by one member of staff. Individualised face-to-face meetings appear to have taken place only when requested by the affected individual and at the discretion of the staff member asked. There is no evidence to suggest that the response was reviewed and used to inform future communications and trust-building activity.

Apologies

Written correspondence demonstrates that senior staff were genuinely concerned when inappropriate access was identified and they regarded the behaviour as unacceptable. Emails and letters for both breaches included expressions of regret and apology.

However, the apologies offered for either breach did not follow a structured approach consistent with NHS Resolution *Saying Sorry* guidance ([Saying sorry \(duty of candour\) - NHS Resolution](#)). In particular, there was no early, clear written apology that:

- Used language that directly recognised the distress caused.
- Explained what was known at that point.
- Acknowledged the impact on the family.
- Set out a commitment to further investigation; and
- Promised ongoing updates.

It is, however, not clear that such an approach would have fully met the family's expectations in 2019.

In 2022, when the family established J4P they sought a public apology as part of a legal settlement, rather than an apology limited to those who had been directly affected.

Updates and ongoing communication

The organisational response to the 2019 breach was framed largely around human resources (HR) and disciplinary processes. By their nature, HR and police investigations are confidential, and it was appropriate that detailed information could not be shared. However, the absence of a wider, clearly documented analysis and plan to address underlying causes limited what staff could communicate beyond disciplinary action.

This contrasted with the family's expectations of detailed involvement in information governance improvements, including scrutiny of audits and technical processes. In response, KEMH shared highly detailed information about audit searches and methods. Rather than resolving concerns, this often generated further technical questions and extended correspondence without providing reassurance.

Complaint handling

Once a formal complaint was submitted, the relevant complaints policy was followed. Senior leadership sought to coordinate responses centrally, rather than leaving individual staff to respond independently. This was appropriate.

The complaint was managed diligently and in good faith, with multiple written responses provided. However, the complaints process was prolonged and difficult to conclude. The policy provided limited guidance on how to manage complaints where responses were not accepted, or where repeated new questions were raised. This made progress challenging for both parties and contributed to entrenched disagreement.

Whilst the terms of reference for this review define those affected by the breach as individuals owed a duty of confidentiality that was not met, it is important to recognise that the impact of the breaches and the response extended far more widely and included:

- 1) Staff who had breached confidentiality
- 2) Staff who were suspected of breaching confidentiality
- 3) Investigators and decision makers
- 4) Wider staff group
- 5) Government, members of the Legislative Assembly and staff
- 6) The public
- 7) External organisations e.g. EMIS, GMC, NMC, Media

Consideration of these perspectives have been incorporated into part B of this report.

Learning and lessons

There was no deliberate attempt to withhold information, however opportunities were missed to:

- Establish a clear engagement plan early on.
- Address both incident management and complaint handling.
- Provide a structured apology and learning narrative; and
- Facilitate staff to contribute to a programme of organisational learning.

These lessons have direct relevance to strengthening future engagement with patients and the public, particularly in the event of further information governance incidents.

Summary of part A: Learning from look back

Overall, the organisation has made meaningful progress since 2019. The improvements implemented following the second breach in 2022 demonstrate wider learning and increasing organisational maturity.

The review found no evidence that KEMH or FIG sought to avoid transparency with patients or the public. Senior staff engaged with affected individuals, responded to complaints and queries, and acted where inappropriate access was identified. A press statement was released in July 2024 summarising the lessons learned from both cases. The breaches were discussed at the Health and Medical Services Committee on multiple occasions.

Key conclusions

Overall, we conclude that:

- The response to the 2019 breach prioritised individual accountability over system-wide learning, which contributed to prolonged dissatisfaction among the complainants.
- Processes followed at the time were defensible but lacked the coordination, structure, and clarity of a serious event analysis because it was not perceived as a serious clinical event.
- The response to the 2022 breach demonstrated learning, with faster escalation, clearer decision-making, and more effective communication with affected patients.
- Opportunities remain to improve governance and better clarify and integrate incident management, complaints handling, and organisational learning and to further align information governance with a patient safety or clinical governance agenda.
- Further progress depends on strategic clarity, sustained leadership focus, and investment in fit for purpose information systems.

Thematic learning

Legislation and policy

UK legislation and NHS policy do not automatically apply in the Falkland Islands. GDPR and the NHS Duty of Candour provide useful reference points, but neither applied directly at the time of the 2019 breach, nor do they apply as statutory requirements now. This has required local interpretation and judgment, sometimes without sufficient clarity.

Complaints and incident management

The 2019 breach may have been managed more effectively had it been treated as a formal incident from the outset, separate to the complaint. Reviewing complaints procedures to provide greater clarity on resolution pathways, redress, escalation, and links to incident management would better support both patients and staff.

Information governance leadership

The Caldicott Guardian role would benefit from clearer definition, training expectations, and formal integration with information governance, clinical governance, corporate governance and incident and complaints management processes.

Systems and audits

Role-based access arrangements have improved, and audit processes are now established. However, legacy IT systems continue to limit what can be achieved. Full replacement of the electronic patient record remains critical to strengthening access controls and assurance and achieving efficiency.

People and culture

Recruitment, induction, training, and contractual requirements have been strengthened. There remains scope to enhance training through practical, scenario-based and face-to-face discussion, particularly for clinical staff, to reinforce confidence about what constitutes appropriate access and disclosure in practice.

Engagement

There is an opportunity to consider whether, and how, the principles of the NHS duty of candour should be formally adopted within local policy to provide clearer expectations for openness, apology, and communication following incidents.

Remaining learning opportunities

Some issues remain only partially addressed and are explored further in Part B of this report. These include:

- Clearer articulation of the practical role and authority of the Caldicott Guardian, including responsibility for incident oversight and escalation.
- Reconsideration of record-locking arrangements, including at the point of death.
- The absence of a clearly articulated and operational link between complaints handling and incident management.

There is also a continuing need to upgrade IT infrastructure to enable modern access controls, strengthen cyber security, and support further improvement in information governance.

Part B: Findings - current information governance & confidentiality

Introduction

This section of the report provides an assessment of the current arrangements for information governance and patient confidentiality at KEMH. It builds on the findings in Part A by examining how the organisation has responded to previous data breaches and how effectively those changes are now embedded.

It draws on evidence from document review, interviews, focus groups, surveys, and site observations. Its purpose is to provide a clear, proportionate assessment of the current position and to inform the recommendations set out later in this report.

Specifically, this section addresses the requirements of the Terms of Reference by:

1. Assessing current practices against relevant NHS information governance standards, where applicable to the Falkland Islands context.
2. Reviewing existing policies, procedures, and guidance and their alignment with recognised best practice.
3. Examining current arrangements for openness and duty of candour.
4. Assessing governance structures, including leadership roles, reporting lines, and the operation of the Caldicott Guardian function.
5. Reviewing arrangements for data storage, access controls, and record lifecycle management across paper and electronic records.
6. Assessing training, awareness, and organisational culture in relation to confidentiality.
7. Reviewing changes implemented following previous data breaches and identifying areas where further strengthening is required; and
8. Scrutinising the current programme of audits and assurance activities.

CQC style inspection 2025

The [CQC style inspection of KEMH](#) in 2025 gives a position of where information governance actions had reached at the start of 2025 prior to the commissioning of this review.

Confidentiality emerged as a significant theme during the inspection, with several findings and recommendations as summarised from the perspective of this review below. Overall, while significant improvements have been made, the CQC style inspection emphasises the need for ongoing vigilance, infrastructure upgrades, and cultural reassurance to maintain patient trust and compliance with confidentiality standards.

CQC Style inspection 2025: Summarised findings relevant to information governance

Data Breaches and Anxiety Among Staff: Previous breaches led to public concern and staff anxiety about accessing records legitimately. While robust measures have since been introduced—such as tiered access rights, mandatory confidentiality training, signed agreements, and spot checks—staff remain apprehensive.

Physical Environment Risks: Feedback highlighted confidentiality issues during consultations in overspill areas separated by curtains, where conversations could be overheard. Inspectors recommended a space utilization review and modifications to ensure privacy.

Audit and External Review: The report advises implementing a regular cycle of confidentiality audits, subject to independent external review, with findings reported to the hospital management board.

Electronic Patient Record System: The current EMIS PCS system is outdated, server-based, and poses governance risks. Inspectors recommend procuring a secure, integrated, cloud-based EPR to improve data security and reduce reliance on mixed paper/electronic records.

Charitable Sector Risks: Information sharing with charities supporting Medical Treatment Overseas (MTO) patients could present confidentiality risks. The report suggests ensuring these organisations understand and comply with data protection obligations.

Duty of Candour and Openness: The hospital promotes an open culture where patients, families, and staff can raise concerns without fear of blame. Senior leaders were described as approachable and responsive, and governance processes include reporting incidents and complaints to HMSC. However, inspectors noted hesitancy among some staff to report incidents and uncertainty about what constitutes a significant event. Recommendations include clearer guidance, mandatory training, and a structured programme of clinical audits to reinforce openness and accountability.

Complaints Handling: While complaints were acknowledged and addressed appropriately, the inspection identified opportunities for improvement:

- Introduce quality assurance measures for serious complaints (e.g., sign-off by senior management).
- Develop a standard operating procedure for handling complaints.
- Ensure learning from complaints is shared systematically with staff.
- Public feedback highlighted concerns about responsiveness and transparency, reinforcing the need for better communication and engagement in the complaints process.

Current perspectives on information governance

This section summarises the reviewers' judgement of how managers, staff, and members of the public perceive the organisation's approach to information governance and confidentiality. It draws on interviews, focus groups, and survey evidence and reflects both progress made and continuing areas of concern.

Managers' perspectives

Managers recognise that the data breaches in 2019 and 2022 were enabled by systemic weaknesses rather than just isolated individual failings. There is also awareness that no system can be designed that is fully protective against a 'bad actor' or misconduct from a member of staff.

Managers widely describe the 2019 response as ad hoc, poorly coordinated, and under governed. In contrast, the handling of the 2022 breach is viewed as a clear turning point, marked by earlier escalation, wider audits, and clearer duty of candour style communication. Information governance arrangements have strengthened since 2022, with more regular access audits, clearer line manager accountability for role-based access, and more consistent induction and regular training. However, they also describe the current position as improving but fragile, with governance still relying heavily on individual expertise and commitment rather than fully embedded systems and culture.

A recurring concern among managers is the level of fear and anxiety among staff. Managers are seeing that fear of breaking rules is undermining staff confidence and decision-making, which may impact safe care and discourage self-reporting. There is strong consensus that staff need clearer, more practical guidance on what constitutes legitimate access, rather than additional layers of policy.

Managers also highlight legacy IT systems as a continuing structural risk and acknowledge that progress on system replacement has been slower than intended.

Patient and public trust is seen as damaged, though partially recoverable, and managers express a clear desire to move from reactive, crisis driven governance to predictable assurance, with routine audit cycles, dashboards, and board level visibility.

Staff perspectives

Staff describe a real cultural shift in how confidentiality and information governance are viewed in day-to-day practice. Compared with the period before 2022, staff report greater awareness and caution when accessing or sharing patient information. Many now actively document reasons for access and are more conscious of audit and oversight.

Peer to peer challenge is increasingly normalised, particularly in relation to corridor conversations and informal disclosure, although this is stronger in some teams than others. Staff widely recognise and accept system improvements, including tighter access controls and improved audit capability, and see these changes, as necessary.

At the same time, staff report ongoing anxiety about "*getting it wrong*." Some describe feeling fearful rather than confident, with concern that a punitive culture could discourage appropriate information sharing and undermine safe care. Uncertainty persists about boundaries, particularly how to balance the duty to share information for care against the duty of confidentiality in multidisciplinary settings.

Staff continue to identify practical risks, including limited confidential spaces, overheard conversations, and residual legacy paper processes. While there is recognition that incident handling has improved since 2022, staff perceive internal communication with them during incidents as slower or less clear and less personal than it should be.

Overall, staff express a strong appetite for practical, face-to-face scenario-based training, concise guidance, visible feedback from audits, and reassurance that decision making will be proportionate and fair.

Patient and public perspectives

Patients and members of the public, especially those affected by the breaches, raise profound concerns about information governance practices. They view confidentiality failures as long standing and cultural, rather than isolated incidents and are much less aware of the developments in information governance that have been made at KEMH since 2022.

In a small community setting, personal familiarity with staff amplifies fear of inappropriate access and increases the perceived harm when breaches occur.

Loss of trust is a dominant theme. Affected individuals describe anxiety about seeking care, avoidance of services, and ongoing emotional harm years after the breaches. Trust erosion is directed not only at individual staff but also at leadership and governance arrangements.

Communication failures are identified as causing more harm than the breaches themselves. Patients describe delays, silence, and learning about events indirectly, including through social media. The handling of the 2019 breach is seen by J4P as dismissive and opaque; the 2022 response is more widely regarded as an improvement but still imperfect, particularly in relation to timing and delivery of notifications.

Patients consistently expect 'duty of candour' style behaviour, including early acknowledgement, honest explanation of what is known and unknown, and personalised contact where harm is likely. Blanket letters without dialogue are viewed as inadequate.

Public confidence is intricately linked to visible safeguards, such as role-based access, routine audits, and clear consequences. Everyday environmental risks, including overheard conversations, staff sharing terminals in clinical spaces and visible paper notes, further undermine confidence.

While engagement improved after 2022, patients and affected people perceive their involvement as episodic and reactive. Their voices have influenced independent reviews and recommendations but are not yet embedded in routine governance, audit oversight, or continuous improvement. Feedback loops are perceived to be weak, with limited visibility of what has changed as a result of patient input.

Summary: Current perspectives

Across all groups, there is recognition that the organisation's approach to information governance and confidentiality has improved, particularly since 2022. Managers and staff see clearer controls and learning, while patients and the public acknowledge progress alongside continued concern. The evidence points to a shared understanding of the problem but differing levels of confidence in follow through. Sustained improvement will require clearer practical guidance, visible leadership, modern IT systems, and more systematic inclusion of patient and public voices in ongoing governance and assurance.

1. Standards, compliance, and good practice

Assessing current practices against NHS information governance compliance review framework (where relevant and applicable to the Falkland Islands).

The Falkland Islands health system recognises and broadly aligns with NHS best practice principles in relation to information governance, particularly the Caldicott Principles, proportionality, accountability, and the balance between the duty to share and the duty to protect confidentiality. Senior managers and clinicians reference NHS standards as a benchmark for good practice, and many of the changes implemented since 2019—such as strengthened audits, clearer access controls, and enhanced training—reflect NHS-informed approaches adapted to the Falkland Islands context.

However, NHS frameworks and legislation do not automatically apply in the Falkland Islands. This has resulted in a selective and incremental adoption of best practice rather than a systematic, end-to-end model. Policies have evolved over time, often in response to specific events, but the overall framework remains complex and, at times, difficult to translate into consistent frontline practice.

Evidence from staff, managers, and the public suggests that the system would benefit from a clearer, locally tailored framework that explicitly reflects NHS best practice while recognising Falkland Islands law, scale, and community dynamics.

There is a need for:

- A clearly articulated local duty of candour policy that sets expectations regarding openness, apology, and communication following incidents. Note that a duty of candour policy and a planned approach to transparency in relation to information governance as described below, are different.
- A concise, practical confidentiality and information-sharing guidance resource that supports staff decision-making in real clinical scenarios 24 hours a day.
- Clearer definition of roles, escalation routes, and accountability within information governance, including the Caldicott Guardian role; and
- Stronger integration between incident management, complaints handling, and information governance assurance.
- Clear integration and alignment of information governance with clinical and corporate governance and particularly incident management, complaints handling and assurance into a single coordinated governance approach.
- An organisational plan for transparency, engagement, and communication with all stakeholders with the aim of demonstrating trustworthiness and feedback loops with stakeholders.
- A tested business continuity plan with respect to information governance.

Overall, the Falkland Islands system demonstrates increasing alignment with NHS best practice in principle and intent. The next step is to consolidate this alignment into a smaller number of clear, practical, and consistently applied policies that provide assurance to patients, confidence to staff, and sustained oversight for the organisation.

2. Policies and guidance on confidentiality

Existing policies, procedures, and guidance in respect of information governance and confidentiality and how these align with best practice in the NHS.

The current information governance policies, procedures, and guidance that we have seen as part of this review include:

1. Information governance policies

- a. FIG Privacy Notice
- b. FIG Data Protection Policy
- c. FIG Code of Confidentiality Policy
- d. Code of Confidentiality Agreement & Guidance
- e. KEMH Access checklist – to approve EOR role-based access to EMIS.
- f. DHSS Complaints Policy
- g. FIG Risk management policy
- h. Incident Reporting Policy
- i. FIG Whistleblowing Policy and Procedure
- j. SEA_SOP [Significant Event Analysis – Standard Operating Procedure]
- k. Information Governance - detailed policy guidance
- l. Directorate of Health & social Service Information Sharing – Public Statement
- m. FIG Acceptable Usage Policy – ICT

2. Records Management Policy & Procedure

- a. Records management principles guide
- b. DHSS Document Records Management Operational Policy 2.0
- c. Corporate Records Retention & Destruction Policy
- d. FIG DHSS Subject-Access-Request-Form
- e. FIG Information system Acceptable Usage Policy 2022
- f. EPR User Audit
- g. Guidance for Access Audits of EPR
- h. IG Record keeping policy.

3. Recruitment, Training

- a. Recruitment & Selection Policy
- b. Induction Policy
- c. Mandatory Training Policy
- d. Recruitment, Selection & Induction Procedure

Existing information governance policies and alignment with NHS best practice

As can be seen above, the Falkland Islands have a large suite of policies and guidance covering information governance, confidentiality, records management, access control, incident reporting, training, and complaints. Overall, these align well with the principles of NHS best practice, particularly the Caldicott Principles, accountability, proportionality, and the balance between information sharing and protecting confidentiality.

The policy set shows the organisation understands what good practice looks like and has sought to reflect NHS standards. In areas such as confidentiality agreements, audit, records retention, and IT use, policy coverage is broadly comparable to NHS organisations.

However, policies are not consistently translated into clear, accessible, practical processes and guidance for frontline staff. Many documents mix policy, process, and guidance, making them harder to use. This is most evident in situations where staff need to balance confidentiality and information sharing in real time (for example, multidisciplinary team discussions, safeguarding situations, medical transfers, or small community dual-role contexts).

As a result, alignment with NHS best practice is stronger at the level of policy intent than in day-to-day usability and lived practice.

There are also structural gaps:

- No overarching framework sets out how policies are created, owned, maintained, and governed.
- No clear mechanism shows how Falkland Islands Government (FIG) policies are assessed for fitness within the DHSS context.
- No clarity on when and how DHSS should locally interpret or implement FIG policies.
- There is no clearly defined approach to data sharing with third parties e.g. Medical Treatment Overseas and third sector organisations or between disparate departments.

The complaints policy for FIG and KEMH should be outside the scope of the terms of reference for this review but has been brought into scope as a result of the 2019 breach response which was largely managed as a complaint.

3. Openness, transparency, and apologies

To assess the current arrangements for duty of candour and openness.

The review found no explicit local duty of candour policy applying to information governance incidents. While elements of candour—such as acknowledgement of error, expressions of regret, and patient notification—were evident in practice, these were applied inconsistently and without a clear, shared framework to align expectations.

In the absence of a codified duty of candour approach, staff and managers lacked clarity about:

- When openness about an incident should be triggered.
- What form apologies and explanations should take.
- How engagement with affected individuals should be structured; and
- How candour should interact with complaints, incident reporting, and disciplinary processes.

This contrasts with NHS best practice, where duty of candour policies provide better certainty for staff and predictable expectations for patients. The lack of an explicit local policy contributed to confusion, inconsistent engagement, and heightened tension following the 2019 breach and was not present to support a professional duty of candour for all registered health and social care professionals. The response to the 2022 breach demonstrated greater openness, indicating learning, but this improvement relied on individual knowledge and was not underpinned by a formal policy framework.

4. Leadership and accountability for information governance

The governance structure/ framework for information governance, and where relevant to the KEMH, within FIG more generally. This may include the placement of the Caldicott Guardian role, and possible future policy development.

Information governance sits within a broader clinical and corporate governance framework at KEMH and FIG, with defined policies for risk management, incident reporting, and significant event analysis. However, evidence suggests that information governance has relied heavily on individual roles rather than embedded systems and overall strategic leadership of information governance is not well described.

The Caldicott Guardian role is established in policy, but its operational authority and visibility are limited. Staff and some managers report little routine interaction with the role, particularly outside core hospital focussed services. There is no clear articulation of whether the role is advisory or decision making, and specifically of:

- The Caldicott Guardian's role in supporting the lawful, ethical, and appropriate use of confidential data and specifically in incident escalation or complaints.
- Their authority in complex information-sharing decisions; or
- Their responsibility for system-wide development, assurance, and learning.
- The Caldicott Guardians role in relation to other confidential information e.g. that of staff and family members and visitors.
- The time and resource available to the Caldicott Guardian, e.g. the creation of a Caldicott decision log and a data disclosure log, access to specialist advice and training, and any potential role for other staff in championing confidentiality.
- How the Caldicott Guardian raises issues to decision makers.
- Whether the Caldicott Guardian is likely to face any conflicts of interest and how these will be resolved or managed.

This differs from NHS best practice, where Caldicott Guardians are visible senior leaders and part of a wider information governance function. They have a clear role covering privacy by design, incident management, information sharing, audit and assurance, and data breach investigations.

The current arrangements limit the role's potential impact and contribute to a perception that information governance leadership is largely the responsibility of the Caldicott Guardian and therefore person-dependent rather than system-owned.

The relationship between FIG and DHSS in the context of information governance is understood by those familiar with it but not well articulated for newcomers and members of the public. There is no organisational chart or drawing showing the relationship and accountabilities between the different elements e.g. Human Resources and DHSS. This is important in terms of understanding the policy framework, policy ownership and how Government policy is interpreted for implementation at KEMH and across health and social care and therefore how policy compliance is measured. Policies do not currently have consistent branding and document control in this regard.

Job descriptions do not all include reference to the role holder's individual responsibility to good information governance within the organisation.

5. How patient information is stored and accessed

The current arrangements in relation to data storage and access controls, for both paper based and electronic records.

KEMH and FIG have established policies and procedures covering records management, retention, destruction, and access control. Audit arrangements and role-based access processes have strengthened since 2019, and staff and managers recognise meaningful improvements, particularly after 2022.

However, legacy IT systems remain a significant constraint. Electronic patient record systems provide only coarse-grained role-based access, limiting the ability to restrict visibility to defined caseloads. System limitations continue to restrict assurance and contribute to anxiety among staff and service users. These are hard to change before the system is upgraded but should be reviewed as soon as possible in the context of re-procurement.

Current practice related to records of deceased patients is not described in policy. The review team were advised that records were not routinely locked because multiple members of the multidisciplinary team need access. This aligns with common UK practice.

Current practice related to the use of the system "confidentiality module," for records clinically judged to be extremely sensitive, is to leave the entire record accessible. This is to safeguard access in emergencies. An extra layer of protection is assumed, but not demonstrated, by having clinical details as attachments rather than integral to the record, thus requiring an additional sequence of deliberate actions to access them and thereby guarding against accidental access (data masking).

Paper records and hybrid processes persist in some services, increasing the risk of inadvertent disclosure, incomplete record keeping and loss of data integrity.

Environmental risks, such as overheard conversations, limited confidential spaces, staff sharing IT monitors in public spaces and visible paper records, were repeatedly identified by staff and patients.

6. Staff training and organisational culture

The current arrangements for training in relation to information governance and confidentiality.

Mandatory information governance and confidentiality training, with assessment of understanding of the training, is in place. As are induction processes and signed confidentiality agreements. This aligns with NHS expectations and represents a clear improvement since 2019.

However, the current training model relies heavily on e-learning, with limited opportunity for discussion of real-world scenarios and meeting individual learning needs. Staff consistently report uncertainty about how policies apply in practice, particularly where professional judgement and ethical decision making is required.

Both staff and managers express a strong preference for:

- Scenario-based, face-to-face training.
- Guidance grounded in real Falkland Islands contexts; and
- Reassurance that proportionate, defensible decision-making will be supported.
- A no blame culture supportive of self-reporting.

The review found evidence that some staff had witnessed, or been involved in, incidents but chose not to report them. No clear reason was identified. However, the reviewers do not consider this to reflect a blame-based culture, as they also heard several examples of good self-reporting practice that should be recognised, encouraged, and celebrated.

7. Changes made since the data breaches

“Changes that have been implemented in respect of previous data breaches and assess what further measures may be recommended to strengthen these.”

Since the 2019 and 2022 breaches, significant improvements have been made, including:

- More regular and structured access audits.
- Clearer role-based access approval processes.
- Accessible e-training and confidentiality re-attestation.
- Policy to allow patients to request audit data on staff accessing their notes; and
- Greater leadership focus on information governance risks.

These changes demonstrate learning and increasing organisational maturity, particularly in the handling of the 2022 breach.

However, the review found no evidence of a single, strategic, organisation-wide reset of information governance. Improvements have instead been incremental and reactive. Further strengthening will require:

- Full implementation and evaluation by stakeholders (staff and public) of recommendations from the 2025 CQC style review. Consolidation of policies into a clear framework with practical guidance and explicit processes.
- Explicit integration of candour, complaints, incidents, and information governance assurance and alignment within a wider governance framework.
- Stronger operationalisation of the Caldicott Guardian role.
- Clear lines of accountability, reporting, and communication for all information governance roles.
- Investment in modern information systems to address structural risk; and
- Consideration of how to demonstrate trustworthiness to all stakeholders.

8. Audit, oversight, and ongoing assurance

“Scrutinise and assess the current programme of information governance audits.”

KEMH has established a structured audit framework for monitoring access to electronic patient records. This is set out in formal guidance and supported by defined criteria for evaluating access, including role-based access, least privilege principles, documentation of access reasons, and explicit prohibitions on accessing family members’ records without authorisation.

Audit oversight sits with the Healthcare Governance Manager, supported by the Data System Administrator. Audit activity is both proactive and reactive, with:

- Routine proactive audits conducted quarterly, to provide ongoing assurance; and
- Reactive audits undertaken in response to complaints, service user concerns and requests, or other intelligence, including police or legal enquiries.

Audits apply primarily to staff accessing electronic clinical systems used within KEMH, including EMIS PCS, pathology, and imaging systems. Social care systems are currently outside the scope of this guidance, reflecting differences in system capability and audit functionality.

Effectiveness of monitoring for inappropriate access

The current routine audit processes to detect inappropriate access represent a significant strengthening of assurance compared with arrangements in place prior to 2019. They are above and beyond any local legislative or policy requirement and, in the opinion of the reviewers, represent the most effective way possible with the current IT system. The introduction of clear audit criteria and routine review of access logs has improved the organisation's ability to identify:

- Unauthorised or suspicious access.
- Repeated or unusual access patterns.
- Evidence of shared logins or inappropriate system permissions; and
- Access to records without a clear clinical justification or legitimate relationship with the patient's pathway.

Where access is identified as potentially suspicious, the process provides for escalation to senior clinical or managerial leadership, further investigation, and, if necessary, referral into disciplinary or criminal processes. Where the audit has been requested by a service user and access is deemed legitimate, service users are informed of the investigation undertaken and its outcome, with support to interpret audit trail data if requested.

In practice, KEMH has also taken preventative system actions, including removing patient sensitive information from appointment views in EMIS, reviewing staff access profiles with line managers, and improving physical access controls within the hospital. These measures complement audit activity by reducing the likelihood of inappropriate exposure in the first place.

However, the effectiveness of audits remains constrained by legacy IT systems, which limit the granularity of role-based access and the precision of audit trails. These constraints are recognised within the organisation and limit the extent to which technical controls alone can prevent misuse. The current legacy IT system is such that the audit process is resource intensive and has no automated alerts for access which is known to be recognised as red flag e.g. same family name.

Audit cycle and use of learning

The formal audit cycle is set out in guidance and includes:

- Quarterly proactive audits.
- Clear processes for receiving and scoping audit requests.

- Defined thresholds for escalation and investigation; and
- Requirements for documentation and retention of audit evidence.

Learning from audits has been used to inform practical changes, including:

- Review and tightening of access permissions.
- Updates to confidentiality policies.
- Delivery of targeted training; and
- Targeted reviews of records management practices in collaboration with the FIG Records Manager.

KEMH also undertakes audits at the request of service users. This audit process is resource intensive but supports transparency and provides reassurance where concerns are raised. However, evidence from interviews and focus groups indicates that feedback loops from audit activity to staff and the public remain underdeveloped. Audits lead to corrective action, but there is less evidence that learning is communicated widely and clearly, limiting their wider preventative value.

Overall Assessment

The current information governance audit programme at KEMH is clearly defined, operationally embedded, and materially stronger than in the past. Routine proactive auditing, clear escalation routes, and defined criteria for assessing access represent good practice and align with NHS principles of assurance and accountability.

Nonetheless, the audit programme is still heavily dependent on:

- Individual roles and discretionary effort rather than system wide capacity.
- Legacy IT systems that limit technical control; and
- Limited visibility of learning outcomes beyond those directly involved,

and is resource intensive. Further strengthening would require better integration of audit findings into organisational learning, clearer communication of audit outcomes, and continued investment in modern systems to support more granular and preventative access controls and release resource for other, more broad information governance related audit controls e.g. procurement, record keeping, lifecycle and retention, clear desk, disclosure logs.

Both FIG and DHSS are currently tolerating a high risk related to its EPR system within its risk management framework. No mitigations are published. The review team requested but have not yet had sight of a tested (audited) business continuity plan with respect to information governance.

The review team requested evidence that the organisation understands and has documented how information is shared with subcontractors and partners, what data is involved, and the contractual arrangements that govern these relationships. However, sufficient evidence was not provided to demonstrate that these data flows and subcontractor arrangements are regularly reviewed or audited.

Audit of information governance controls e.g. policy statement standards and effectiveness of training is not yet fully established. However, external audit against GDPR standards at KEMH Ward, Hillside and Community Support team was undertaken in February 2023. Actions were

assigned and reviewed in March 2024 with significant actions seen to be completed. The standards have not yet been re-audited.

Audit of organisational adoption and performance against the eight Caldicott principles is not yet evidenced.

Although there is evidence of oversight via senior management team meetings where information governance subjects are raised, the review team saw no evidence of ongoing system oversight in the form of a dashboard or basket with metrics and KPIs to demonstrate, to staff and the public, ongoing information governance assurance.

The review highlights that, although a powerful tool to identify process control performance, audit alone will not improve information governance and needs to be part of a comprehensive, holistic development plan and over reliance on audit as a control mechanism can result in a culture of fear and blame.

Recommendations

“To provide specific, achievable recommendations for improvement that are implementable within the context of the Falkland Islands and to advise how these can be independently audited.”

“Assess what changes in relation to records management, information governance and confidentiality would be recommended to be considered by the organisation.”

The recommendations we make following our review are summarised in the executive summary at the front of this report.

Appendix A: Terms of reference

Introduction

This appendix provides the full Terms of Reference (ToR) governing the external review of information governance and confidentiality practices at KEMH.

The ToR outline the purpose, scope, method, responsibilities, and expected outputs of the review, and were approved by the Executive Council on 14th October 2025 after having been agreed between the two parties.

Terms of reference:

Terms of Reference in relation to external review of information governance and confidentiality practices at the KEMH

Background

In 2019 and then again in 2022 it was discovered, following enquiries from patients about access to their confidential medical records, that members of staff at the King Edward VII Memorial Hospital (KEMH), with no connection to those specific episodes of care, and without any justifiable reason to view those episodes of care had been doing so. In some cases, this related to the records of deceased patients, well after their death. In both cases internal investigations, disciplinary and criminal prosecutions followed. Despite similarities, there were also a number of differences in how the two cases were handled, including differences in the scope of the investigations, how affected patients were notified and the route by which matters were reported to the Police.

Since these matters were raised concerns in relation to information governance and confidentiality have continued to be raised by a group of affected individuals known as Justice4Patients. This culminated in January 2025 with the group seeking redress via means of a constitutional claim at the Supreme Court of the Falkland Islands.

Introduction

In order to provide an objective assessment of the handling of previous data breaches and current information governance and confidentiality practices at the KEMH, it has been agreed to commission an independent, external review. It is intended that the review will provide the basis for future improvements and developments in these areas, as well as provide transparency to the public in relation to these matters, through a publicly available report being published. Whilst the focus of the review is on the KEMH and its response, consideration will be given as to how the breaches were handled across the wider administration of the Falkland Islands Government (FIG).

Independent nature

Although being sponsored and paid for by FIG, it is the express objective of this review to be both external and independent of the FIG. No employee of the FIG, current or otherwise should seek to influence the review's findings and written report other than to comment on matters of factual accuracy before its publication. The final report will be published without redactions as far as possible. Any redactions required under FIG's Data Protection Policy will be notified to

Justice4Patients. As laid out below it is an obligation of the review team to be both impartial and neutral.

Qualifications and experience of review team

It is anticipated that the independent review will be carried out by a team of two experienced individuals with suitable background and experience in the UK. Agreement on the appointment of the reviewers will be reached between the Director of Health and Social Services and Justice4Patients. If agreement cannot be reached within three months of the date of agreement of these terms of reference, FIG reserves the right to request its Health and Medical Services Committee (HMSC) to agree the appointment.

Ideally, the reviewers are required to possess the following attributes:

- At least one reviewer to have substantive experience as a Chief Information Officer (CIO) or Caldicott Guardian (5 years' plus) ideally within the healthcare sector.
- At least one reviewer to have demonstrable experience of conducting investigative reviews (ideally within the healthcare sector)
- Experience of auditing, reviewing compliance and report writing.
- understanding of best practise in information governance and data protection within the NHS
- Clear understanding of best practice in the NHS in relation to patient access to audit trails of user access to patient records
- Clear understanding of regulatory and professional standards in healthcare.

Main aims

The main aims of this external, independent review are to;

1. Assess the response by KEMH/FIG to the previous data breaches, discovered in 2019 and 2022, including lessons learned from these events.
2. Provide an overview and assessment of the current arrangements at the KEMH in relation to information governance and patient confidentiality.

Additional aims

- To provide a balanced overview to the public of the current arrangements in relation to information governance and confidentiality at the KEMH via the means of a public report.
- To provide the basis for an achievable local action plan to drive further improvements in relation to information governance and confidentiality in KEMH and more broadly across FIG.
- To promote openness and transparency in relation to information governance and confidentiality at the KEMH in order to promote public reassurance in these matters.

Sponsor

The sponsor of this review with oversight of the review is Andrea Clausen the Chief Executive. Detailed matters relating to the review will be dealt with by the Director of Health and Social Services, who is commissioning the review on behalf of the KEMH, and the FIG.

Scope of review

Critically review the approach to detecting, assessing, managing and reporting data breaches in relation to previous data breaches, and in addition to review;

1. The circumstances in which previous data breaches occurred and identify contributing or causative factors to these breaches.
2. The decision-making in relation to the handling of previous data breaches, and requests for audit trails within the KEMH and in the FIG corporate decision-making structure (including decision making about referral to the Police).
3. The processes followed in respect of each previous data breach, and whether these complied with policies which were extant at the time or relevant deemed best practice in the NHS, including the duty of candour.
4. Identifying any missed opportunities which would have improved the quality of the response in each instance and aligned the response with recognised best practice.
5. Understand improvements made after the 2019 data breach and identify further learning opportunities with respect to previous data breaches, including those already acted upon by the KEMH, and those which would further strengthen information governance for the future.
6. Review the approach taken by the KEMH and FIG in relation to engagement with those affected by the data breaches to identify any lessons learned or missed opportunities, particularly in relation to whether NHS best practice was followed for appropriate apologies, keeping those affected victims updated and offering support.

Critically review the current status of information governance at the KEMH, including;

1. Assessing current practices against NHS information governance compliance review framework (where relevant and applicable to the Falkland Islands)
2. Existing policies, procedures and guidance in respect of information governance and confidentiality and how these align with best practice in the NHS.
3. To assess the current arrangements for duty of candour and openness.

4. The governance structure/ framework for information governance, and where relevant to the KEMH, within FIG more generally. This may include the placement of the Caldicott Guardian role, and possible future policy development.
 5. The current arrangements in relation to data storage and access controls for both paper-based and electronic records.
 6. The current arrangements for training in relation to information governance and confidentiality.
 7. Changes that have been implemented in respect of previous data breaches and assess what further measures may be recommended to strengthen these.
 8. Scrutinise and assess the current programme of information governance audits.
- To ensure that any significant new concerns in relation to information governance and confidentiality are appropriately raised, including externally to the KEMH, if required.
 - To provide specific, achievable recommendations for improvement that are implementable within the context of the Falkland Islands and to advise how these can be independently audited.
 - To meet with relevant members of the senior management team and individual members of staff, both in a planned and opportunistic manner to provide an overview of the understanding and practical approach to information governance and confidentiality in the organisation generally.
 - To provide the opportunity for interested members of the public including those affected by the data breaches to meet the review team to discuss their concerns, and where appropriate (ensuring anonymity), include a summary of these findings in the report.
 - Assess what changes in relation to records management, information governance and confidentiality would be recommended to be considered by the organisation.
 - To provide a publicly available report of the review's findings and recommendations.

Obligations

The KEMH will:

- Provide an initial information pack of all relevant documents and material to the reviewers before arriving in the Falkland Islands to ensure they have the necessary background information to be able to maximise the time in the Falklands.
- Provide all additional documentation and materials requested and required by the review team in a timely manner.
- Ensure, as far as reasonably practicable, that any relevant data that might have been deleted from the Government records system is recovered by the IT Dept.
- Discuss and agree with the review team how they will engage with Justice4Patients before their arrival in the Falkland Islands.
- Take all reasonable steps to seek the participation of relevant current and former KEMH/FIG staff in relation to any questions asked by the reviewers and will ensure key members of current staff are available to meet with the reviewers (by remote access if necessary)
- Act upon any significant concerns which are raised, and in relation to new information about data breaches, follow the process defined in an annex to the Code of Confidentiality.

- Ensure an action plan is drawn up on receipt of the external report, which will then be approved and reported on in the open section of the HMSC in timely manner.

The review team will:

- Remain impartial and neutral throughout.
- Provide a factual and balanced report, using professional judgement to recognise elements of best practice that should be promoted and preserved in addition to making recommendations for improvement.
- Raise any significant concerns that emerge and ensure they are satisfied that they are being appropriately acted upon.
- Conduct further investigations in relation to any matter within the included terms of reference they deem appropriate.
- Provide the KEMH and Justice4Patients group equal opportunity to review the draft report prior to publication to allow an opportunity to comment on any material factual inaccuracies accepting neither party has the right to change the report after it is presented.

Resources

The KEMH will provide the necessary budget to cover the cost of the review.

Logistics

The KEMH will arrange and pay for the flights, transfers and accommodation of the reviewers. The KEMH will provide any necessary administrative support.

It is anticipated that the review team should carry out an initial review of the documents followed by a minimum of one week on location in the Falkland Islands in order to follow up with investigations and meet with all relevant individuals.

Timelines

To be agreed with review team once appointed

Outcomes

The following outcomes are expected;

- Written, unredacted (any redactions required under FIG's Data Protection Policy will be notified to Justice4Patients), publicly available report. This will be available on the FIG website, included in the open section of the Health and Medical Services Committee (HMSC), and publicised via a press release.
- Published action plan, developed by KEMH and discussed with external parties within six months from receipt of the report. This will be included in the open section of the HMSC.
- Ongoing work in relation to and monitoring of the action plan in the open section of HMSC meetings.
- Recommendation as to future review/ governance arrangements.

Appendix B: Public apology

Introduction

This appendix provides the full text of the public apology delivered by the Government on 28th August 2025 in relation to the matters examined in this review.

Including the apology in full ensures transparency, supports the public record, and provides essential context for the findings and recommendations discussed in the main report.

Context of the apology

The Government delivered this apology following:

- Concerns raised by service users and the wider community.
- A Consent Order accepting they had breached the Constitutional Rights of those members of the Justice4Patients group who had their medical records illegally accessed; and
- A commitment to acknowledge harm, rebuild trust, and affirm the rights and dignity of affected individuals.

This apology forms part of a broader effort to strengthen accountability and demonstrate a commitment to improvement.

Full text of the public apology

“The Falkland Islands Government and KEMH wish to apologise to those in the community affected by the two data breaches that occurred at the KEMH in 2019 and 2022. We offer a wholehearted and unequivocal apology for this breach of privacy by two former KEMH employees and for FIG’s failure to proactively manage and follow up these breaches at the time.

When confidential information is held and used by an organisation, a duty of trust exists whereby service users can reasonably expect their data to be held securely and only viewed and used for legitimate reasons which are directly linked to the operation of the organisation holding that data.

For some individuals affected, the data breaches have caused emotional distress and, in some cases, may have deterred those individuals from accessing certain services due to a loss of trust. The individual circumstances of each person affected are different, meaning that for some individuals these breaches may have caused considerable emotional distress which may have regrettably impacted on other aspects of their lives. The Falklands Island Government and KEMH deeply regrets any emotional distress caused and any subsequent impacts of this.

Good practice when things go wrong is to apologise immediately. We accept that those affected by the first data breach had to wait 4 years for any detailed apology despite the KEMH and FIG being aware that their right to confidentiality had been breached. Whilst the KEMH and FIG have since made previous apologies; it is now recognised that a meaningful apology which reflects the full impact of the data breaches on all members of the community and complies with best practice has not previously been made.

In 2019 and then again in 2022 it was discovered, following enquiries from patients about access to their confidential medical records, that members of staff at the KEMH, with no

connection to those specific episodes of care, and without any legitimate or justifiable reason to view those episodes of care had been doing so.

In relation to the data breach, which was discovered in 2019, whilst the KEMH did initiate its own internal conduct and disciplinary investigations, the KEMH, and the FIG did not report the case to the Police. This was wrong. Affected patients were left to report matters to the police themselves, inevitably causing further distress. The case subsequently went to Court and during the trial it was found that the KEMH was unable to show that sufficient training and guidance on confidentiality had been given to this employee and their use of the computerized medical records system was not audited. We apologise for not referring this matter to the Police and for failing to train and monitor this former employee properly in relation to the confidentiality of data, data protection and information governance.

Whilst following the data breach which occurred in 2019 some limited changes in procedures and processes to strengthen data protection arrangements at the KEMH were made these regrettably did not prevent a further data breach in 2022. Members of the Justice4patients group identified an employee who was again misusing the access rights they had been granted as part of their role to access confidential medical information with no justifiable reason for doing so. We apologise that more robust actions to address the findings in the first case were not taken as it could have significantly reduced the likelihood of this recurrence.

In 2022 when the second data breach was discovered, it was determined that around 290 members of the community had their confidential medical records accessed after thorough investigation by the KEMH and RFIP. Members of the community who had been affected were written to by the Director of Health and Social Services at the time and a successful prosecution took place. Since that time, we acknowledge that until a press release in September 2024, there was no follow-up and update to members of the community on what actions had been taken. We also recognise that further efforts should have been made to more fully understand the impacts of these breaches on the community. We accept that communication with those affected was very limited and that no support was offered to those affected.

It is now approximately 6 years since the first data breach and nearly 3 years since the second, and we are very sorry that communication and apology over that timeframe has not followed what is considered to be “best practice” in these situations.

Members of the community who feel that their concerns in relation to these data breaches have not been heard, or recognised, and who wish to receive a personal apology may request an appointment with the Director of Health and Social Services by calling 28017 or e-mailing pa.dhss@kemh.gov.fk

We hope that the community will accept this apology as it is meant, as a starting point to improve trust in confidentiality at the KEMH. The KEMH are seeking to arrange an independent external review to learn from previous breaches and to improve on current practices. The terms of reference for this review have been developed in consultation with the representative group Justice4Patients. This review will seek to understand how data breaches have been handled by the KEMH and FIG, what further lessons can be learned, and what additional measures can be taken to further strengthen information governance and improve our response when things go wrong. Those impacted by the data breaches will have the opportunity to meet with reviewers

to detail the impact it has had on them. The results, recommendations and action plan will be made public.

It remains the case that individuals who have queries or concerns about access to their electronic medical records may make enquiries with the KEMH who will seek to address these in the most appropriate way. We recognise that patients have the ability to request an audit of who has accessed their medical records and have the results shared with them in a way that is compatible with best practice in the NHS and our own policy.

Finally, we wish to acknowledge the role of members of the public in raising concerns and bringing these issues around information governance to our attention.”

Delivery and publication details

- **Date delivered:** 30th October 2025
- **Delivered by:** Dr. Andrea Clausen, Chief Executive, Falkland Islands Government
- **Format:** Delivered at meeting of Legislative Assembly, Press conference, Press statement

Notes on usage in the review

The apology is reproduced in full to:

- Preserve the wording exactly as delivered.
- Allow readers to understand Government commitments in their proper context. support evaluation of subsequent actions and changes.

Appendix C: Caldicott Principles

Introduction

This appendix outlines the Caldicott Principles. The Caldicott Principles provide a framework for the protection and appropriate sharing of patient information for use by all staff. Although developed within the UK NHS, the principles are widely recognised as best practice and are used internationally to support lawful, ethical, and appropriate handling of personal confidential data in health and social care settings.

The principles underpin many information governance policies in the Falkland Islands and are referenced throughout this report.

Overview

The Caldicott Principles were first established following a review led by Dame Fiona Caldicott in 1997. They have since been reviewed and updated, most recently in response to public consultation to reflect increasing expectation of transparency¹.

The principles apply to all personal confidential data, regardless of format (electronic or paper), and to all staff, clinical and non-clinical, who have access to patient information.

The Eight Caldicott Principles

1. Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

2. Use confidential data only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

3. Use the minimum necessary personal confidential data

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

4. Access to personal confidential data should be on a strict need-to-know basis

¹ Department of Health (2020) Caldicott Principles: a consultation about revising, expanding and upholding the principles. London: Department of Health. Available at: <https://www.gov.uk/government/consultations/caldicott-principles-a-consultation-about-revising-expanding-and-upholding-the-principles>

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

6. Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

7. The duty to share information for care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8. Inform patients and service users about how their information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Practical application

In practice, the Caldicott Principles require staff to exercise professional judgement. Decisions about access and sharing should balance confidentiality with safety, necessity, and proportionality. Where uncertainty exists, staff should seek advice through line management, governance leads, or the Caldicott Guardian.

The principles also underline the importance of:

- Clear role-based access controls.
- Routine audit and monitoring of access.
- Prompt escalation of concerns; and
- A just culture that supports learning and openness rather than blame.

The Caldicott Guardian Role²

Caldicott Guardians provide leadership and informed advice on complex matters involving the use and sharing of confidential health and care information. They help their organisations to uphold the Caldicott Principles and ensure that confidential information about health and social care service users is used ethically, legally, and appropriately, especially in situations where there may be areas of legal and or ethical ambiguity. The Caldicott Guardian promotes good information governance throughout their organisation, using the principles to encourage and facilitate decision making with documented rationale in the best interests of patients, service users, and their care.

² Department of Health and Social Care (2022) National Data Guardian guidance on the appointment of Caldicott Guardians, their role and responsibilities. London: Department of Health. Available at: <https://www.gov.uk/government/publications/national-data-guardian-guidance-on-the-appointment-of-caldicott-guardians-their-role-and-responsibilities>

Appendix D: Documents reviewed

Governance structures & oversight

- Health and Medical Services Committee [HMSC]: Terms of Reference and Guidance
- Record of the Meeting of the Legislative Assembly Held at the Falkland College, Stanley. [26 September 2024]
- Directorate of Health and Social Services Strategy and Action Plan 2025-2029
- Health and Social Services Directorate Organisational Structure (established posts)
- Chief Medical Officer Job Description
- Chief Nursing Officer Job Description - draft
- Director of Health and Social Services Job Description
- Hospital Manager Job Description
- Healthcare Governance Manager Job Description

Governance: Overarching framework

- Summary of FI Legislation Relevant for information governance
- Falkland Islands Government, Data Protection Policy (December 2020)
- Falkland Islands Government, Health and Social Services Directorate Information Governance Policy Strategy (September 2012) - superseded
- Falkland Islands Government, Health and Social Services Directorate. Information Governance Strategy Overview Policy Document (September 2019)
- FIG Access to Health Records Ordinance 1995
- Falkland Islands Government, Health and Social Services Directorate. Information Governance - Detailed Policy & Guidance [June 2019]

Information governance & data protection

- FIG DHSS Information Governance policy (March 2013)
- Falkland Islands Government Privacy Notice – Directorate Health & Social Services [no date]
- Health and Social Services Directorate. Sharing of Information Statement [no date]
- Falkland Islands Government, Health and Social Services Directorate, Code of Confidentiality (February 2025)
- Falkland Islands Government, Health and Social Services Directorate, Code of Confidentiality (August 2022) - superseded
- Falkland Islands Government, Health and Social Services Directorate, Code of Confidentiality (October 2014) - superseded
- FIG DHSS Code of Confidentiality Policy 2014 - superseded
- Falkland Islands Government. Acceptable Usage Policy - Information and Communications Technology (December 2023)

Records & information management

- FIG DHSS Information Governance Records Management Policy [March 2014]
- FIG DHSS Information Governance: Records Keeping Policy April 2014
- FIG Corporate Records Management - Records Management Principles Guidance (2022)
- DHSS Health Records Management: Operational Policy (August 2023)
- FIG DHSS. Data Protection Subject Access Request Form - to request access to health record.
- Medical Treatment Overseas. Information Booklet (September 2025)
- FIG Corporate Records Retention Schedule: Health & Social Services Directorate (September 2025)
- Invitation to Tender to provide the Falkland Islands Government with an Electronic Patient Record (EPR) System (September 2023)

- Award of Contract to supply the Falkland Islands Government with a Meals on Wheels Service (October 2024)
- Award of Contract to supply Cleaning Services to Tussac House (July 2024)
- EMIS Confidentiality Policy Guidance
- Audit Report & Recommendation Tracker Data Protection Assessment – Health & Social Services Directorate February 2023
- Findings of Audits: Staff Access to Patient Records [i. 1/09/24 to 31/12/24; ii. 01/01/25 to 31/03/25; iii. 01/03/25 to 31/05/25; iv. 01/06/25 to 31/09/25; v. 01/10/25 to 18/12/ 25]
- Falkland Islands Government. Acceptable Usage Policy - Information and Communications Technology (April 2022)
- Audit of Electronic Records Access; Criteria for Evaluating User Access in EPR System (April 2024)
- Falkland Islands Government, Health and Social Services Directorate. Guidance for Access Audits of Electronic Patient Records (February 2025)
- Falkland Islands Government, Health and Social Services Directorate. Information Governance Records Keeping Policy
- EMIS training handout. Audit Trails

Risk, incident & assurance

- Falkland Islands Government, Health and Social Services Directorate, Incident Reporting Policy (November 2021)
- Falkland Islands Government. Risk Management Policy and Implementation Strategy [no date]
- Falkland Islands Government, Health and Social Services Directorate, Complaint Compliments and Comments Policy (April 2025)
- Falkland Islands Government Whistleblowing Policy (April 2025)
- Falkland Islands Government Whistleblowing Procedure (April 2025)

Workforce

- Falkland Islands Government, Health and Social Services Directorate, Code of Confidentiality Agreement for signature (February 2025)
- Code of Confidentiality Brief Guide
- Code of Confidentiality Brief Guide (2014) - superseded
- FIG Recruitment, Selection & Induction Policy
- FIG Recruitment, Selection & Induction Procedure
- Falkland Islands Government, Health and Social Services Directorate. Staff Induction Policy
- Using e-Learning for Healthcare for Mandatory Training
- Falkland Islands Government, Health and Social Services Directorate. Mandatory Training Policy (December 2023)
- KEMH New starter Access Form
- Falkland Islands Government, Health and Social Services Directorate. Procedure for Undertaking a Significant Event Analysis (September 2021)

Assurance / Evidence Artefacts

- KEMH Senior Management Team minutes (8 October 2025)
- KEMH Report Summary of complaints in 2025
- KEMH Report Summary of Risk Register in 2025
- Extract summary of current live incidents on DHSS risk register (February 2026)
- Patient satisfaction survey results 2020
- King Edward VII Memorial Hospital Inspection Report (January 2025)

Complaint and Its Management

- Summary of data (documents) April 2019 to August 2023: Regarding response to Data Breach 2019
- Summary statement of timeline from J4P
- Email from HGM to all KEMH staff [23 December 2015]. Regarding code confidentiality
- Email from HGM to all KEMH staff [30 January 2018]. Regarding code confidentiality

2019

- Statement [23 January 2019] from Healthcare Governance Manager which staff had access named patient record (RE).
- Record of Interview with named member of staff ARR: Investigation into Breach of the Department of Health and Social Services Code of Confidentiality Policy
- Email from HGN to Hospital Manager & HR [20 January 2019] Regarding data from Audit on access clinical records in first breach
- Letter to named member of staff [24 January 2019] Invite to an Investigation Meeting
- Letter to named member of staff [24 January 2019] Invite to an Investigation Meeting
- Email from HCM to KEMH manager [24 January 2019] confirming staff who had left KEMH user access inactivated.
- Letter to named member of staff [25 January 2019] Invite to an Investigation Meeting
- Investigation report [28 January 2019] regarding named member ARR of staff
- Investigation report [28 January 2019] regarding named member of staff KW
- Letter to named member of staff KW [29 January 2019] Invite to an Investigation Meeting
- Record of Interview with named member of staff ARR [28 January 2019]: Investigation into Breach of the Department of Health and Social Services CoC Policy
- Witness Statement [28 January 2019] from named member of staff.
- Email from Director HSS to J4P [28 January 2019] Response to J4P email 26 January 2019.
- Email exchange from HGM to Manage and CMO [29 January 2019] regarding data from first audit, and role AG as point of contact.
- Email from Healthcare Governance Manager [30 January 2019]. Audit of named records and access by named member of staff
- Witness Statement [30 January 2019] from named member of staff.
- Email from HGN to Hospital Manager [30 January 2019] Regarding data from Audit on access clinical records in first breach
- Investigation report [31 January 2019] regarding named member of staff AC
- KEMH Terms of Reference [31 January 2019] Disciplinary and Capability Investigation into named member of staff.
- Witness Statement [31 January 2019] from named member of staff DC regarding allegation of a separate information breach.
- Statement from named member of Staff [31 January 2019] Investigation: Breach of the Department of Health and Social Services Code of Confidentiality Policy
- Record of Interview with named member of staff KW [31 January 2019]: Investigation into Breach of the Department of Health and Social Services CoC Policy
- Letter from J4P to Director HSS [2 February 2020] Response to letter 21 November 2019
- Email from J4P to CMO [7 February 2019] Regarding information breach and reply [8 February 2019]
- Email exchange from J4P to CMO [7 February 2019] and response [8 February 2019] Regarding actions being taken in response to breach.
- Email exchange HGM and CMO [14 February 2019] regarding actions in response to first data breach.
- Letter from AG to J4P [15 February 2019] Legal view The Access to Health Records Ordinance 1995, wider policy and case law context
- Witness Statement [16 February 2023]. Statement to Police by HGM regarding second data breach
- Email exchange FIG HR with KEMH [26 February 2019] regarding actions following breach.
- Email from J4P to PA Director HSS [1 March 2019] asking for update in investigation information breach.

- Letter from Director HSS to J4P [6 March 2019]: Response to letter 1 March 2019. Update on progress investigating breach
- Email HR to Hospital Manager [21 March 2019] Regarding actions from first breach.
- Email from Hospital Manager [1 April 2019] Regarding actions from first breach
- Email from AG to Director HSS [10 April 2019] Advice Note. Interpretation of the Access to Health Records Ordinance 1995 with respect to rights to access data
- Letter from J4P to Hospital Manager [11 April 2019]. Request for data on who accessed records named person.
- Letter from J4P to Director HSS [12 April 2019] Response to Director HSS letter 11 April 2019
- Letter from J4P to Hospital Manager [11 April 2019] asking for data on who access medical records.
- Letter from Hospital Manager to J4P [16 April] regarding request for access data.
- Letter from Director HSS to J4P [25 April 2019] Response to J4P letter 12 April 2019.
- Emails from J4P to Director HSS [25 April 2019] acknowledge receipt not yet responded to letter from J4P on 18 April as out of office.
- Letter to J4P from Director HSS [26 April 2019] Confirming unauthorised access of named persons medical records and explaining steps being taken.
- Copy of Letter to second person in J4P from Director HSS [26 April 2019] Confirming unauthorised access of named persons medical records & steps being taken
- Letter from Director HSS to J4P [29 April 2019] Update - concluding Internal Investigation by HR and proposed steps to review IG.
- Email from Director HSS [1 May 2019]. File notes on information governance and response to breach.
- Email from AG to J4P [1 May 2019]. Regarding referral of issue to Police
- Letter from Hospital Manager to J4P [8 May 2019] Follow up to a meeting / conversation to confirm information regarding whether an individual member of staff had accessed their medical records.
- Letter from J4P to Director HSS [10 May 2019] Covering Letter to Formal Complaint Concerning Inappropriate Access to Electronic Medical Records by KEMH Employees
- Letter from J4P [10 May 2019]: Complaint in Relation to the Inappropriate Access of Electronic Medical Records by Employees of the Falkland Islands Government (FIG) Working in the Department of Health and Social Services
- Email from Director Human Resources (FIG) to Director HSS [24 May 2019]. Summarising HR actions in response to information breach.
- Email exchange KEMH [26 May 2019] Collating response to J4P complaint questions.
- Email exchange KEMH [28 May 2019] Collating response to J4P complaint questions.
- Email from Director HSS to incoming Director HSS and HCM [May 2019] taking Review Governance arrangements.
- Email from AG to Director HSS [10 June 2019]: collating information in response to J4P complaint
- Letter from Director HSS to J4P [17 June 2019]. Response to complaint 10 May 2019 duplicate - also from P4J
- Speech MLA Elsbey to Legislative Assembly [25 July 2019]
- Letter from J4P to Director HSS [25 July 2019]. Response to letter 17 June 2019
- Verbatim Record of Interview AG and MLA Spink [August 2019] Regarding Data Protection
- Letter from Director HSS to J4P [5 September 2019]: Response to letter 25 July 2019
- Letter from J4P [12 September 2019] Consulting MPS regarding information breach
- Reply from Medical Protection Society to J4P [3 October 2019]
- Letter from J4P to Director HSS [9 October 2019]: Response to letter 6 September 2019
- Letter from Director HSS to J4P [9 November 2019]: Response to letter 9 October 2019
- Email from Director HSS to J4P [21 November 2019]. Response to letter 9 October 2019

2020

- Letter from J4P to Director HSS [2 February 2020]. Response to letter 21 November 2019
- General information statement [no date] from Healthcare Governance Manager to Police on EMIS and information governance arrangements
- Statement to Police [13 June 2020] on EMIS Governance from Healthcare Governance Manager regarding named member of staff KW

- Letter from J4P to Clinical Governance Manager [5 October 2020] regarding aspects of complaint
- Letter from J4P to Chief Medical Officer [5 October 2020] regarding aspects of complaint
- Letter from J4P to Chief Nurse [5 October 2020] regarding aspects of complaint
- Letter from J4P to Director Health & Social Care [5 October 2020] regarding aspects of complaint
- Audit Results [16 October 2020] Access to electronic records – Audit which staff accessed an Individual EMIS record.

2021

- Court Determination R v Williamson 2021
- Email from J4P to GMC [2 January 2021] Regarding management of information breach and role of clinician
- Reply from GMC to J4P [18 January 2021] Initial Response
- Letter from J4P to CMO [26 March 2021] Requesting audit trail on who has accessed for named person's records.
- Email from Hospital Manager to J4P [20 April 2021] Regarding queries about EMIS audit data
- Email from Director HSS to J4P [29 April 2021] in response to J4P emails to CMO, CNO, Governance Manager co-ordinating response from KEMH
- Reply from GMC to J4P [15 June 2021] Final Response
- Email from J4P to NMC [23 June 2021] referring concerns to UK Nursing and Midwifery Council. Response from NMC [19 October 2022]
- Email from J4P to NMC [24 June 2021] referring concerns to UK Nursing and Midwifery Council. Response from NMC [19 October 2022]
- Letter from Director HSS to J4P [28 June 2021] response to letters 25 June 2021, to CEX, CMO, CNO, HGM, letter 2 Feb 2021 and closure of J4P complaint
- Email from Director HSS to J4P [11 August 2021] in response to J4P request for meeting with Hospital Manager regarding access to medical records.
- Letter from J4P to FIG CEX [19 August 2021] Appeal about the management of, and closure of J4P complaint
- Letter from CEX [1 November 2021] response to appeal, following meetings 1 September 2021 and 15 October 2021

2022

- Email from Director HSS [27 October 2022] regarding identification of second data breach
- Letter from Director HSS [4 November 2022] regarding EMIS audit and follow up to correspondence 1 November 2022.
- Email from Director HSS to KEMH leads [29 November 2022] regarding actions in response to second data breach and letter to affected patients.
- Email from Director HSS to senior staff [1 December 2022] actions in response to second breach
- Letter from Director HSS [5 December 2022] Formal notification that records have been found to have been inappropriately accessed.
- Email from Director HSS [8 December 2022] to team proposing co-ordinating response to complaint through Director HSS
- Director HSS Letter to Patients Notification of Unauthorised Access to Clinical Notes (Nov 2022)

2023

- Witness statement to Police from HGM [16 February 2023] Regarding KEMH information governance management.
- Email from FI Police to KEMH [30 March 2023] notifying of charging decision in relation to second breach.
- Email Director HSS to HGM [11 May 2023] regarding actions & audit following second breach.

- Application from J4P [17 March 2023] Request for Copy of an individual's Medical Records From 15/08/2017 - 19/03/2023
- Court Determination R v Stevens [22 May 2023]
- Letter from J4P to Governor [12 July 2023] Regarding named patient's care, management of a related complaint, and information breach
- Letter from GMC to J4P [27 July 2023] in response to referral to GMC by J4P
- Terms of Reference for the Targeted Patient Record Access Review - KEMH [22 August 2023]
- KEMH Record of Decisions and Lessons Learned After 2021 and 2023 Staff Court Cases (August 2023)
- Facebook Chat Statement from J4P [Screen capture September 2024]
- Letter from Governor to J4P [15 November 2023] Response to letter 1 November, and meeting in July
- Letter from Waverley Law to CEX [1 December 2023] Letter before Claim against FIG under Constitution
- Targeted Patient Record Access Review- KEMH Response [19 December 2023]
- Penguin News: Maternity Care Questions Public Meeting. Quote from J4P (November no year)
- Private Eye Interview with J4P [no date]
- Summary KEMH IGM of Patient emails in response to 2022 Breach notification letter

2024

- Facebook Chat Feed from J4P [Screen capture January 2024]
- File note from P4J [2 January 2024] Asking for line-by-line explanation of findings in EMIS audit linked to named patient record.
- Letter from Director HSS to EMIS Health [10 January 2024]: Asking for clarification details of IT audit of individual's clinical record.
- Letter from EMIS to Director HSS [18 January 2024]: Regarding aspects of EMIS audit
- Email from Data Systems Analyst to Director HSS [19 January 2024] explaining details regarding SQL coding for Audit searches in EMIS audit.
- Letter from Director HSS to J4P [25 January 2024] Response to J4P letter 18 January 2024 Regarding aspects of EMIS audit
- Letter from Director HSS to J4P [26 January 2024]: Response to J4P letter 22 January. Regarding aspects of EMIS audit.
- Letter from Director HSS to EMIS Health [24 January 2024]: Asking for clarification details of IT audit of individual's clinical record.
- File note Data Systems Analyst [5 February 2024] Analysing results EMIS Audit compared to KEMH audit.
- Letter from Director HSS to J4P [7 February 2024]: Response to J4P letter 22 January and Follow up to Letter from Director HSS 26 January. Regarding aspects of EMIS audit.
- Letter from J4P to Director HSS [19 February 2024]: Response to Director HSS letter 7 February Regarding aspects of complaint.
- Briefing Note KEMH internal document [9 March 2024]: Summary timeline
- J4P Excerpt from Public Meeting [April 2024]
- FI TV Interview Director HSS [(June 2024) Regarding actions taken since information breaches
- Director HSS Press Release: Update on Data Handling and Confidentiality at the KEMH (July 2024)
- Press Statement FIG [10 September 2024] Update on data handling and confidentiality at the King Edward VII Memorial Hospital
- Press Statement FIG [12 September 2024] Clarification on previous press statement.
- Terms of Reference in relation to External Review of Information Governance and Confidentiality Practices at the KEMH

2025

- Press Statement FIG [27 January 2025] KEMH Inspection Report
- Announcement by J4P [21 January 2025] Regarding File of Claim with Supreme Court
- Letter from visiting UK MP to FI Governor [12 March 2025] Regarding J4P's concerns.

- Email Data Systems Administrator to Director HSS [20 March 2025] with attachments summarising Police Investigation
- Supreme Court of the Falkland Islands [20 October 2025] Amended Consent Order
- FIG Press Statement [27 October 2025] Terms of Reference Agreed for Information Governance Review
- Falkland Island Government Press Statement [28 August 2025]. Falkland Islands Government Apologises for Hospital Data Breaches
- FIG and KEMH Public Apology in relation to data breaches [2025]

Appendix E: Information governance policy & practice analysis

Purpose of appendix

This appendix provides a structured assessment of information governance (IG) arrangements at KEMH/FIG using NHS best practice as a reference point. It supports the findings presented in Part B of this report and should be read alongside that narrative assessment.

The analysis identifies strengths, gaps, and areas of development, recognising that the organisation has made incremental improvements since 2019, particularly following the 2022 breach, but has not yet established a fully integrated and mature IG framework.

Benchmark framework

There is no single mandated IG policy set. NHS organisations operate within a comprehensive governance framework that integrates:

- Data protection and confidentiality (GDPR, common law duty of confidence)
- Caldicott Principles
- Records management standards
- Data security standards (NDG)
- Organisational accountability and board assurance
- Cybersecurity

NHS organisations are expected to self-assess their arrangements using the NHS Data Security and Protection toolkit: [Data Security and Protection Toolkit](#) and/or [Principle A1 Governance | National Cyber Security Centre](#) and develop improvement plans where standards are not met. Compliance with DSPT and the Cyber Assessment Framework (CAF) is monitored by NHS England.

In the Falkland Islands, these do not apply directly but are used in this review as a benchmark for good practice, consistent with the approach taken in the main report.

Overall maturity assessment (Aligned Position)

The current position can be summarised as:

- Broad policy coverage is in place, reflecting NHS principles,
- Significant improvement since 2019, particularly in training, audit, and access control,
- Reliance on incremental development rather than strategic design,
- Fragmented governance framework with unclear integration across domains,
- Strong intent but variable operationalisation in practice,
- Undeveloped approach to Cyber risk management.

Governance framework and accountability

Expected Standard	Current Position
A clearly defined IG framework	Governance structures and leadership roles exist in policy. But no overarching framework.
Formal leadership roles (e.g., Caldicott Guardian, SIRO equivalent) defined, appointed and public facing	The Caldicott Guardian role is defined, but not yet fully embedded or consistently visible and understood. Caldicott function not well described
Board-level oversight and assurance with clear accountability and reporting	Board-level assurance mechanisms exist but lack clear line of sight from audit to risk to mitigation and assurance.
Integrated links between IG, clinical and corporate governance, risk, and complaints	Accountability across IG, complaints, records, and risk is not clearly demonstrated to be integrated or aligned with the patient safety agenda
	Overall, reviewers assess the governance framework exists in part but lacks definition, is incomplete and not fully embedded. Governance remains person-dependent rather than system-led.

Information governance policy framework

Expected Standard	Current Position
Coherent suite of policies, procedures, guidance, and training (Data Protection, Confidentiality, Information Sharing, SAR, Breach Management, Business Continuity, Acceptable Use, Third-party agreements, IAR, ROPA, Privacy Notices, DPIA, Access Controls, Mandatory training)	Broadly aligned. Large suite of policies exists and reflects NHS principles.
Defined ownership and version control	Documents are fragmented and inconsistently structured.
Clear distinction between policy, procedure, guidance, and training	Limited clarity on how FIG corporate policies apply within health and social care. Documents conflate policy, process, and guidance

Expected Standard	Current Position
Practical usability for frontline staff	No overarching framework explaining how policies fit together.
	Overall, document control, ownership and review inconsistent. Strong coverage but weak coherence impacting usability.

Confidentiality and data protection

Expected Standard	Current Position
Clear confidentiality policy aligned to Caldicott principles	Code of Confidentiality and Data Protection Policy in place with Caldicott Principles incorporated. Training, agreements, and awareness have improved since 2019.
Defined lawful basis for data use	Not strictly applicable but transparency around data use could include a local approach
Embedded data protection practices	Application in practice is variable; documentation does not fully support operational consistency.

Information sharing and external interfaces

Expected Standard	Current Position
Formal data sharing agreements	Recognition of need for sharing; public-facing statements exist. Limited evidence of systematic, formalised data sharing agreements.
Clear lawful basis and accountability	Not strictly applicable but transparency around data use could include a local approach
Oversight of third-party and cross-border sharing with documented rationale, risks, and mitigations	Oversight of third-party arrangements and non-health partners not fully defined. Information sharing between departments (e.g., health/social care, dentistry/mental health) not well described.

Subject access and transparency

Expected Standard	Current Position
Clear SAR process and legal framework	No statutory GDPR-style SAR in Falkland Islands law; local access and audit mechanism introduced.
Transparency around access and data use	Innovative audit but not part of a comprehensive rights-based framework. There is little public information on IG; policies and dashboards are not published; Caldicott Guardian contact details are not published.

Audit, monitoring and assurance

Expected Standard	Current Position
Comprehensive IG audit framework	Quarterly audits on staff accessing records. Wider audit programme limited
All policy controls and areas in scope	Audit focused on record access rather than full IG system performance.
Prioritisation for high-risk areas	Improvement since 2019 but no comprehensive IG assurance framework.
Defined KPIs and reporting cycles	FIG 2023 data protection audit is a strength.
Learning integrated into governance	Not evidenced

Incident management and learning

Expected Standard	Current Position
Integrated incident and near-miss reporting and learning system	Incident reporting and SEA procedures exist but were not used for these breaches.
Clear linkage to IG, complaints, and governance	Improved response in 2022 breach acknowledged.
Tested business continuity/disaster recovery plan	Historical absence of systematic IG incident handling; weak integration with complaints and learning; unclear recovery capability.

Records management

Expected Standard	Current Position
Full lifecycle management of records	Record management policies in place, including retention schedule.
Clear accountability, controls, monitoring, audit and KPIs	Hybrid record risks observed (paper records on desks).
Alignment with retention standards	Not evidenced
Alignment with professional integrity/availability requirements	Not evidenced
Applies to paper, digital and AI-generated records	Not evidenced

Workforce, training, and culture

Expected Standard	Current Position
Recruitment/selection policy describing confidentiality requirements	Not evidenced
Pre-employment checks (ID, DBS)	Pre-employment checks in place.
Mandatory role-based training and competency assessment	Mandatory e-learning and induction strengthened post-2019. Heavy reliance on e-learning; staff uncertainty; appetite for scenario-based training. Practical case discussion and ethical problem-solving recognised but not formally facilitated.
Role-based access and least privilege	Evident but limited
Strong reporting and learning culture	Some self-reporting evident but not universal.
Individual learning needs analysis and CPD	Not evidenced

Expected Standard	Current Position
Development of a local “just culture”	Not evidenced

Cross-cutting themes

Across all domains, five consistent themes emerge:

- Incremental improvement rather than strategic redesign
- Strong policy intent but weak operational translation
- Fragmented governance and accountability
- Reliance on individuals rather than embedded systems
- Structural constraints driven by legacy IT.

Consolidated gap statement (Aligned to Report)

The key gaps are not absence of policy, but lack of integration, clarity, and system maturity:

- No fully articulated end-to-end IG governance framework
- Limited integration between IG, complaints, incidents, and risk
- Incomplete definition and operationalisation of leadership roles
- Absence of a coherent assurance model beyond access audits
- Weak formalisation of data sharing governance
- Ongoing dependency on legacy systems

Conclusion

KEMH/FIG demonstrates a clear understanding of information governance principles and has made meaningful progress since 2019. However, the current system remains fragmented in design, variable in implementation and constrained by infrastructure.

The next phase of development requires consolidation into a smaller, clearer, and system-led framework, aligned to the findings and recommendations as set out in the main report.

Appendix F: Interviews & key lines of enquiry

Introduction

This section summarises the interviews conducted, both in person on the island and remotely via *Microsoft Teams* and sets out the key lines of enquiry that informed these discussions.

Summary of Interviews

Name	Job title
On island in-person interviews	
John Woollacott	Director of Health and Social Services
Mandy Heathman	Chief Nursing Officer
Janette Vincent	Healthcare Governance Manager
Chloe Anderson-Wheatley	Corporate Records & National Archives Manager
Artur Zalewski	Data System Administrator
Amelia Bone	Acting Practice Manager
Dr Rebecca Edwards	Chief Medical Officer
Simon Young	Attorney General
Momtaz Begum	Head of Legal Services
Andrew Potts	Hospital Manager
Lisa Martin	Former Data System Administrator
Colin Martin-Reynolds	Governor of the Falkland Islands
Dot Gould	Member of the Legislative Assembly
Stacy Bragger	Member of the Legislative Assembly
Dr Andrea Clausen	Chief Executive, Falkland Islands Government
Leigh Reid	Head of Care Services
John Birmingham	Former Member of the Legislative Assembly
Dr Anette “Neti” Murphy	Clinical Psychologist
Dr Bernadette Paver	Member of the public (Justice4Patients)
Dr Barry Elsby	Member of the public (Justice4Patients)

Anya Bull	Member of the public (Justice4Patients)
A small number of members of the public were interviewed.	
Off-island interviews via Teams	
David O'Neil	Previous Director of Health and Social Services
Ann Hunt	Previous Hospital Manager
Mandy Whittingham	Previous Director of Health and Social Services
Tom Bale	Previous Director of Health and Social Services
Focus groups, on island, in-person	
• DHSS Managers & Senior staff • KEMH Ward staff • Staff members • Affected members of the public. • General Public	
Media slots	
FIRS (radio), FITV, Penguin News	

Key Lines of Enquiry

The review team used the Terms of Reference to develop Key Lines of Enquiry. These were used to structure surveys, interviews and focus groups.

Assess the Response by KEMH/FIG to the Previous Data Breaches.

Terms of Reference	Key Questions
Circumstances and contributing factors.	What were the circumstances that led to the breaches in 2019 and 2022? What organisational, technical, or cultural factors contributed to them? Specifically consider themes: people, process, and technology.
Decision-making in handling breaches	How were decisions made about handling the breaches (e.g., scope of investigations, referral to the Police, patient notification)?
Compliance with clinical records access policies and NHS best practice at the time.	What were the policies, training, culture and (best) practice in place at the time. What was in place for NHS at the time? To what extent were the responses aligned with existing policies at the time?
Missed opportunities or weaknesses in response.	Were there any missed opportunities to strengthen the response or mitigate impact?

Lessons learned and changes implemented since 2019.	What lessons were identified, and which of these have since been acted upon?
Government engagement with affected individuals (apologies, updates, support).	How did the Health Authority and Government communicate with affected individuals (apologies, updates, support)? Was this consistent with best practice and Falklands Policy or NHS policy?

Provide an Assessment of the Current Arrangements at the KEMH.

Current Information Governance (IG)

Terms of Reference	Key Questions
Existing policies, procedures and guidance	What are the current IG policies, procedures and guidance?
Assessing current practices	How do current IG practices compare with local guidance? To what extent does the Falklands system recognise NHS best practice; and what policies should be in place?
Current arrangements for duty of candour and openness.	What are the current policies in terms of Duty of Candour?
The governance structure/ framework for information governance	What are current IG arrangements? How does the role of the Caldicott Guardian function? How does it align with clinical governance, incident and risk management frameworks.
Current arrangements for data storage and access controls to clinical records	What arrangements are in place for clinical record storage and access? [full record lifecycle]
Arrangements for training on IG and confidentiality.	What training on IG and confidentiality is provided? How do FI assure that it is well understood and applied by staff?
Changes that have been implemented after previous data breaches	What changes have been made in terms of IG of clinical records since the breaches in 2019 and 2022?
Scrutinise and assess the current program of information governance audits	What oversight audit and monitoring are undertaken? How effective are current processes for monitoring inappropriate access to records?

	What is the audit cycle and how are lessons learned/practice changed?
Perspectives from staff, management, and public (including affected patients).	How do staff and managers perceive the organisation's approach to IG and confidentiality? What concerns or insights do patients and members of the public (including those affected by breaches) raise about IG practices? How effectively are their voices incorporated into governance and improvement planning?
Keeping the public informed about information governance arrangements.	What reporting mechanisms are in place to keep the public informed? What information is available to the public and service users about how their information is used and managed?
What further measures may be recommended to strengthen these.	What gaps, risks, or unresolved issues remain in IG and confidentiality practices? [People, process, technology] What measures would be most effective and achievable in strengthening IG of clinical records locally?

Appendix G: Interview findings

Overview

This appendix summarises what participants said across interviews, including staff, managers, senior leaders, government representatives, and service users. It reflects how people described the circumstances, responses, and impact of the breaches in their own terms.

While there are differences in perspective, there is strong consistency in the themes raised.

Circumstances and Contributing Factors (What People Described)

Across interviews, participants repeatedly pointed to the same starting point: systems and controls were too open without sufficient checks and balances in place. Managers and system staff described access controls as unclear or inconsistently applied. There were examples given of staff learning systems *“on the job”* without formal training.

Service users described concerns about confidentiality going back several years, including rumours of inappropriate access to records.

The small community context was raised in almost every discussion. Participants described how *“everyone knows everyone,”* with staff and patients often connected socially or through family networks. This was seen as increasing both the temptation to access records and the impact when it happened. One view captured this clearly: information *“travels very, very fast”* in the community.

Several participants also described uncertainty about what counted as legitimate access. This applied particularly in situations where staff had multiple roles providing cover across different departments and settings.

Handling of the Breaches (How People Experienced It)

Descriptions of the 2019 response were consistently critical. Staff, managers, and service users all described a lack of structure and coordination.

- Managers and clinical leaders said, *“there was no pathway”* and that the response felt *“very ad-hoc.”*
- Service users described long periods without information, with one stating *“there was literally nothing”* in terms of updates.

There were also shared views that escalation was unclear. Some interviewees said it was not obvious when police should be involved or who was responsible for leading the response.

In contrast, the 2022 breach was widely described as more organised. Staff and leaders pointed to faster action, including immediate suspension and early police involvement. Participants also referred to the scale of the response, with around 250 to 300 people identified and notified.

However, service users and some staff said that communication still fell short. Although letters were sent, several described a lack of follow-up and ongoing uncertainty. One account referred to *“silence... no update” after initial contact.*

Policies, Training and Practice (What People Experienced in Reality)

Across all groups, there was general agreement that policies existed but were not consistently used or understood.

- Staff described signing confidentiality agreements but not always receiving practical training. One service user summarised this perception as people “*not being told what confidentiality means, just signing a paper.*”
- Managers also highlighted gaps in induction and training, particularly for non-clinical roles.

At a system level, government and corporate staff described progress after 2019, including the development of privacy policies and retention schedules. However, they also noted that adoption within services was uneven and sometimes resisted by staff.

Several interviewees described a wider gap between policy and practice. Policies were seen as present “on paper” but not consistently embedded in daily work.

Weaknesses and Missed Opportunities (Reflections from Participants)

Participants from all groups identified missed opportunities after the 2019 breach.

- Government and leadership interviews highlighted that systems and policies were not strengthened quickly enough at that point. One comment noted that “*the policy itself didn’t change.*”
- Managers described the organisation as “*reactive and not very proactive*” in identifying and managing risks.
- Service users were particularly clear on this point. Several said that earlier, more open action could have resolved concerns much sooner. One described that if action had been taken immediately, the situation “*would have been sorted in 6–8 weeks, not 6 years*”.

Across interviews, there was also recognition that audit processes were limited before 2022. Breaches were often identified only after concerns were raised, rather than through routine monitoring.

Engagement with Affected Individuals (What People Said About Communication)

Service users provided the clearest and most consistent feedback in this area.

In relation to 2019, they described limited communication, lack of transparency, and difficulty obtaining information. Some reported having to piece together information themselves to understand what had happened.

For 2022, views were more mixed. Participants acknowledged that letters were sent and that some individuals were offered more detailed information on request. However, concerns remained about:

- Lack of ongoing updates
- Unclear explanations
- Distress caused by how and when communication was delivered.

Some interviewees also described longer-term impacts, including reduced trust and hesitation about engaging with services.

Changes Since 2019 (What People Have Noticed)

Participants across all groups recognised that changes have been made since the breaches.

Staff and managers described improvements in access controls, including more structured and tiered access arrangements. Audit processes were also described as more regular and more visible.

Government and corporate interviews highlighted wider developments, including new policies, working groups, and a stronger focus on data protection.

Some service users also noted improvements, particularly in more recent engagement with senior leaders. There were examples of individuals being invited to discuss concerns directly, which was seen as a positive shift.

At the same time, not all impacts were positive: staff described increased anxiety about accessing records, even when appropriate, reflecting uncertainty about expectations and possible consequences.

Overall Narrative from Interviews

Taken together, the interviews describe a system that, prior to 2022, was widely seen as under-controlled, with unclear rules and limited oversight. The 2019 breach is described as poorly handled, with lasting consequences for trust.

The 2022 breach is consistently described as a turning point, where the organisation responded more decisively and transparently. However, participants also make clear that improvements are still in progress and not yet fully embedded.

Across all perspectives, the same core themes recur:

- Electronic patient record access was too broad without sufficient checks in place to train staff and ensure understanding and compliance.
- Audits on staff accessing records were too limited and reactive.
- Policies were not fully understood in terms of practical implementation.
- Communication in the response to the information breaches and management of the specific complaint was not strong enough.

At the same time, there is recognition that awareness has increased, systems are improving, and there is greater willingness to address these issues openly.

Appendix H: Focus group findings

A total of five focus groups were conducted between 28–30 January 2026, involving approximately twenty-four participants across staff, management, and members of the public.

These included senior managers, ward staff, general staff, and patients / public. Several participants noted that they had more than one interest in the issue – often as both members of staff and patients.

Circumstances and Contributing Factors

- Focus groups revealed several positive factors within the organisational culture. Staff consistently described a supportive workplace where colleagues “*get along well*,” maintain professionalism, and feel able to engage in open conversations about confidentiality. This collaborative atmosphere has fostered constructive peer-to-peer challenge, with many staff reporting they feel “*confident about calling out*” unsafe discussions in public areas.
- Senior managers highlighted progress since 2019, including improvements such as improved training, tighter access controls, strengthened information-governance structures and increased monitoring.
- Against this backdrop, however, the focus groups also identified cultural and practical challenges that contributed to confidentiality breaches. Staff and patients described the impact of small-community dynamics, where personal familiarity is common and informal information sharing can feel normalised.
- Longstanding assumptions of ‘trust-based’ access further blurred boundaries. Patients reported overhearing conversations and seeing open paper notes, pointing to environmental risks.
- Staff also expressed anxiety about unclear expectations, which sometimes resulted in both over- and under-sharing of information.

Decision-Making in Handling Breaches: 2019 & 2022

- Participants identified positive developments in how incidents are handled over time. Senior managers noted that later breaches benefited from improved internal coordination and stronger technical controls, reflecting a more structured approach to containment. Affected patients also acknowledged that, when offered, direct conversations were valued and signalled a shift toward more personal and compassionate engagement, even if this was not applied consistently.
- However, participants also described significant challenges in earlier organisational responses. Staff and senior managers agreed that initial communication was delayed, with some staff learning about incidents through social media rather than formal channels. Affected patients reported receiving impersonal letters and insufficient apologies, which contributed to feelings of being dismissed.

- Perceptions of inconsistent treatment of staff based on seniority further undermined trust. While technical responses improved over time, communication pathways were still seen as slow or unclear, limiting confidence in the organisation's overall approach.

Compliance with Policies & NHS Best Practice (at the Time)

- Staff and managers recognised that post-2022 system changes—such as refined access controls, clearer audit trails, and EMIS improvements—brought the organisation closer to NHS best practice expectations. They also reported proactively documenting reasons for accessing notes, showing increased accountability and adherence to confidentiality principles.
- Improvements post-2022—enhanced access controls, consolidated audit trails—were noted by senior managers.
- However, they also described feeling unclear as to how to apply policies in practice. Frontline staff still struggled with clarity on information-sharing rules, particularly during ward rounds and interdisciplinary discussions.

Missed Opportunities / Weaknesses

- Key weaknesses identified included lack of early transparent communication during breaches, insufficient training, unclear role-based access, and environmental risks such as open discussions at reception.
- Patients highlighted failures in communication (letters not arriving, lack of follow-up). Staff cited limited spaces for confidential conversations and ongoing system fragmentation. Organisational follow-through on previous recommendations was perceived as weak.
- While weaknesses around communication, documentation and environmental risks were noted, staff also demonstrated strong examples of self-policing—actively challenging corridor conversations and discouraging informal access to patient information, even when it was once common practice. This represents an important shift toward safer working norms.

Engagement with Affected Individuals

- Affected patients felt organisational communication lacked empathy and clarity. They described the response as lacking meaningful apology. They recommended direct, personal communication such as phone calls, better updates on actions taken, and clear opportunities for dialogue.
- Staff acknowledged the emotional impact on both patients and themselves, emphasising the damage in a small community.
- Although affected patients expressed dissatisfaction with aspects of communication post-breach, some participants valued opportunities to give feedback in structured sessions such as the focus groups themselves. Staff echoed the importance of learning from patient experiences and welcomed more direct dialogue as a form of improved organisational engagement.

Lessons Identified & Actions Implemented Since 2019

The focus groups identified multiple examples of positive progress, including:

- Improved audit functionality allowing clearer monitoring of inappropriate access.
- Stronger access controls and moves away from broad Y-drive visibility.
- Increasing IG awareness, with staff demonstrating more caution and conscious decision-making when accessing records.
- Better digital infrastructure and optimism about future system enhancements.
- Growing appetite for meaningful IG training, with staff requesting scenario-based, practical sessions—indicating cultural readiness for improvement.

For the future, senior managers outlined improvements in digital infrastructure, access controls, and audit trail capability. Staff recognised better IG awareness, greater accountability, and more cautious data handling.

However, cultural change remains ongoing. Both staff and patients called for clearer guidance, realistic action plans, and visible progress reporting. Continued investment in training, system upgrades, and community transparency was seen as essential.

Appendix I: Public survey

Introduction and what the survey covered

The survey asked members of the public to reflect on their recent experiences of using KEMH services, including:

- Whether they believed their personal information was handled responsibly
- How confident they felt that their information was kept confidential
- Their overall trust in how KEMH managed patient information

The survey was open from **16th January 2026 – 20th February 2026**.

Participation, use of findings and confidentiality

The survey was anonymous, with no personally identifiable information collected and no way to link responses to individual participants. All findings were reported in aggregated form and contributed to the independent public report. To support accessibility, the survey was translated into Shona and Spanish; however, no responses were received in either language. An optional free text section was included to allow participants to share additional information.

Public survey summary

The public survey, based on **168 respondents**, found widespread concern about how personal health information is managed by KEMH and a significant erosion of trust within the community. While most respondents (93%) had accessed health or care services recently, many reported limited understanding of what information is held about them and how it is used or shared. A majority were not informed about data use, did not know how to access their own records, and had never discussed confidentiality with staff. This is not too dissimilar from the NHS evidence as The Health Foundation conducted a survey which found 68% of the public trust hospitals and awareness is low, with only 61% saying they know ‘very little’ or ‘nothing at all’ about how the NHS is using the health data it collects³.

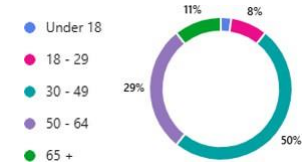
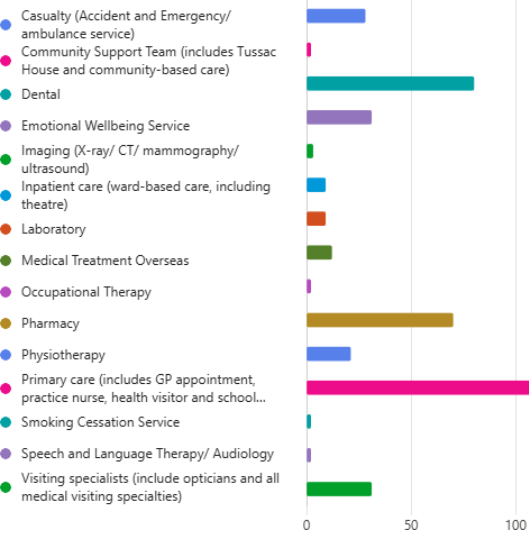
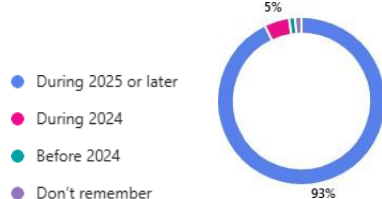
Views on trust and confidence were divided across most topics, including public trust in KEMH to protect information, confidence that only appropriate staff access records, and whether information is treated as private. Although most respondents had not personally experienced confirmed unauthorised access, perceptions of risk and mistrust were high, particularly in the context of recent data breaches.

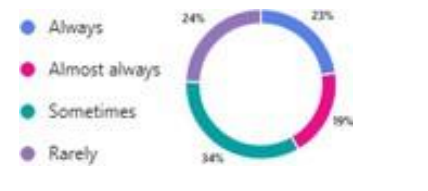
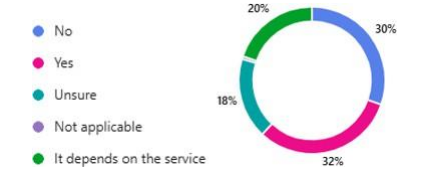
Qualitative responses reveal that confidentiality issues are widely perceived as cultural and systemic rather than isolated incidents. The most common concerns relate to normalised gossip and casual sharing of patient information by staff, overly broad access to medical records, clinical leaders not holding staff to account or providing sufficient role modelling, and physical environments that allow sensitive conversations to be overheard. Small community dynamics were seen as amplifying harm, making confidentiality failures more damaging than in larger settings. Many respondents described serious emotional and behavioural impacts, including fear, shame, loss of trust, and avoidance of healthcare – especially mental health services. While a minority defended KEMH and praised individual staff professionalism, the overall picture is of

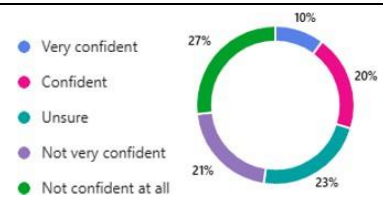
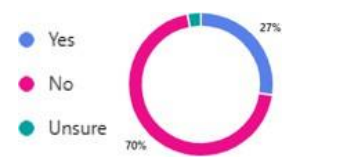
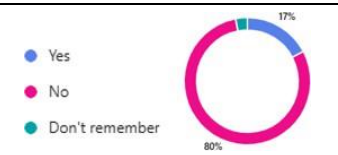
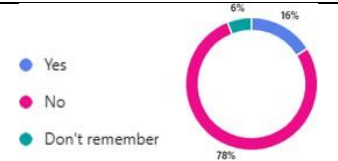
³ Health Foundation (2023) *NHS must protect and build public's trust in its ability to safely handle health data, report argues*. Press release, 24 November. Available at: <https://www.health.org.uk/press-office/press-releases/nhs-must-protect-and-build-public-s-trust-in-its-ability-to-safely>

a divided community and a service facing urgent need for cultural change, stronger governance, clearer communication, and more robust systems to rebuild trust and protect patient confidentiality.

Survey Questions and Answers

Question	Answer	Graph
1.What is your age group?	< 18 years 2% 18-29 years 8% 30-49 years 50% 50-64 years 29% 65+ 11%	 Legend: - Under 18 18 - 29 30 - 49 50 - 64 65 +
2. Which services do you use the most? You may choose up to three.	Top three services used: - Primary Care - Dental - Pharmacy	 Legend: - Casualty (Accident and Emergency/ ambulance service) - Community Support Team (includes Tussac House and community-based care) - Dental - Emotional Wellbeing Service - Imaging (X-ray/ CT/ mammography/ ultrasound) - Inpatient care (ward-based care, including theatre) - Laboratory - Medical Treatment Overseas - Occupational Therapy - Pharmacy - Physiotherapy - Primary care (includes GP appointment, practice nurse, health visitor and school...) - Smoking Cessation Service - Speech and Language Therapy/ Audiology - Visiting specialists (include opticians and all medical visiting specialties)
3. When did you last access health or care services (see a health or care professional) from KEMH?	During 2025 or later 93% During 2024 5% Before 2024 1% Don't remember 1%	 Legend: - During 2025 or later - During 2024 - Before 2024 - Don't remember

4. Do you know what information KEMH keeps about you?	No 51% Yes 38% I was told, but don't remember 4% No, but I know how to find out 8%	
5. Were you informed about how your personal health information would be used, and who it would be shared with?	Yes clearly 7% Yes somewhat 10% No 73% Don't remember 7%	
6. Do you know how to access information that is held about you?	Yes 32% No 51% Unsure 15% Not relevant 2%	
7. Do you feel your information is respected as private?	Always 23% Almost always 19% Sometimes 34% Rarely 24%	
8. Do you trust KEMH to look after information about you?	No 30% Yes 32% Unsure 18% Depends on the service 20% Not applicable 1%	

9. Do KEMH handle patient information responsibly?	No 30% Yes 28% Unsure 26% Depends on the service 17%	 - No - Yes - Unsure - It depends on the service
10. How confident are you that only staff involved in your care access your records?	Very confident 10% Confident 20% Unsure 23% Not very confident 21% Not confident at all 27%	 - Very confident - Confident - Unsure - Not very confident - Not confident at all
11. Have you ever been advised that your health and care record has been accessed by somebody who should not have done so?	Yes 27% No 70% Unsure 3%	 - Yes - No - Unsure
12. Have you ever asked a member of staff about what happens to the information you tell them?	Yes 17% No 80% Don't remember 3%	 - Yes - No - Don't remember
13. Has a member of staff ever spoken to you about what happens to the information you tell them?	Yes 16% No 78% Don't remember 6%	 - Yes - No - Don't remember
14. What improvements would you suggest to strengthen confidentiality and the way KEMH manages and protects information? 115 responses, Respondents recommended strengthening confidentiality through a fundamental cultural and leadership shift, supported by tighter controls and clearer accountability. Many described a normalised culture of inappropriate information sharing, particularly casual gossip among staff and long-standing employees, limited consequences for breaches, and poor oversight. Concerns were also raised about overly broad access to medical records, with calls for stricter role-based permissions, better monitoring, and stronger IT security to reduce unauthorised or accidental access. Physical environments such as open reception and waiting areas were seen as ongoing confidentiality risks, alongside gaps in training and awareness, especially for reception and administrative staff, leading to inconsistent practices. While some respondents felt staff		

did their best, others emphasised that repeated breaches have damaged public trust and that KEMH must visibly demonstrate transparency, respect, and a genuine commitment to protecting patient information to rebuild confidence.

15. Is there anything else you would like to share confidentially with the reviewers?

101 responses reveal a sustained erosion of trust in KEMH's ability to protect confidentiality, driven not only by the two major breaches but by years of normalised gossip, inappropriate access, and weak accountability across staff levels. Issues are widely perceived as cultural and systemic, amplified by small-island dynamics and blurred professional boundaries. Many respondents report fear, shame, trauma, avoidance of essential care, and anger towards leadership and governance, while a minority (7%) maintain trust in clinical staff and view concerns as overstated. Overall, the findings point to a divided community, a workforce under emotional strain, and an urgent need to rebuild confidentiality culture at behavioural, clinical leadership, and system levels.

Appendix J: Staff survey

Introduction

The staff survey asked respondents to reflect on their experiences of using and handling patient information as part of their work. It sought feedback on:

- Current policies and guidance relating to patient confidentiality
- Training and support for information governance
- Day-to-day practices and behaviours affecting confidentiality
- Organisational culture and confidence in handling patient information

Staff perspectives were essential in understanding what was working well in practice and where improvements may be required to demonstrate publicly that patient information is handled in a trustworthy and responsible way.

The survey was open from **16th January 2026 – 6th March**. Note this was extended by a couple of weeks to encourage more staff participation.

Participation, Use of Findings and Confidentiality

Participation in the survey was voluntary and took 8–10 minutes to complete. A total of 41 responses were received and analysed. Staff views were central to informing the review's recommendations, ensuring they were practical, realistic, and supportive of those responsible for managing patient information on a day-to-day basis. As staff members were also users of local health and care services, respondents were additionally invited to complete the General Public Survey if they wished, to share their perspectives as service users.

The staff survey was completely anonymous. No identifiable information was collected, and responses could not be linked to individual participants; the reviewers had no means of identifying who provided specific comments. All responses were combined and reported in aggregated form as part of the independent public report. An optional free-text section was included to allow staff to share additional information they felt the reviewers should consider.

Staff Survey Summary

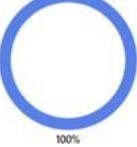
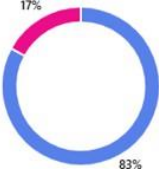
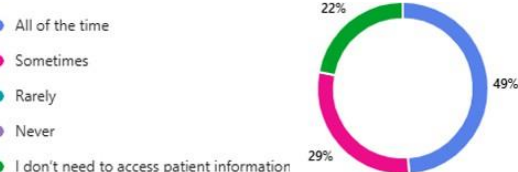
A total of **41 survey responses** were received and analysed, with most respondents having regular direct contact with patients or the public and routinely handling patient information. Overall, staff demonstrated a strong understanding of confidentiality requirements, with high levels of training completion and awareness of how to keep patient information safe and how to raise concerns. Respondents identified people and human behaviour as the greatest risk to confidentiality, followed by environmental factors, technology, and processes. Common risks included corridor conversations, misaddressed emails, accessing incorrect patient records, and challenges associated with working in a small, close-knit community where staff and patients often know one another.

While staff highlighted many examples of good information governance practice, there was strong consensus on the need for further improvements. Key themes included investment in a modern, integrated electronic patient record system; better physical environments that support privacy; stronger access controls and governance; and more consistent, practical training. Respondents also emphasised the importance of a supportive, no-blame culture that encourages reporting and learning from mistakes.

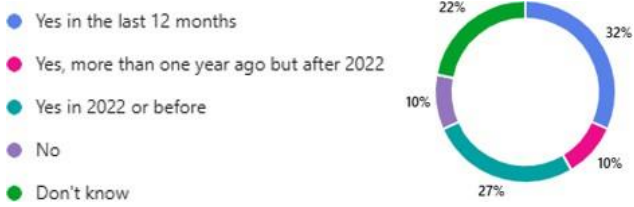
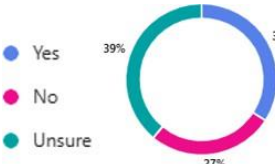
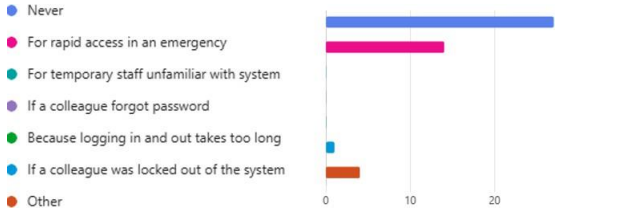
Many described the emotional impact of recent confidentiality breaches and public scrutiny, expressing a desire for clearer leadership, cultural change, and sustained improvements to help restore confidence and support both staff and patients.

Survey questions and answers

Question	Answer	Graph														
1. What is your primary role?	21 Clinical 4 Administrative and Clerical 5 Management 8 Professional, Scientific, and Technical (ex-scientist, lab techs, pharmacist, psychologist, radiographer, engineers, IT, and data professionals, etc), 1 Estates and Ancillary 2 Other	<table><tr><td>Clinical</td><td>21</td></tr><tr><td>Administrative and Clerical</td><td>4</td></tr><tr><td>Management</td><td>5</td></tr><tr><td>Professional, Scientific and Technical (ex scientist, lab techs, pharmacist, psychologist, radiographer, engineers, IT, and data professionals, etc)</td><td>8</td></tr><tr><td>Estates and Ancillary (ex maintenance, cleaning/housekeeping, porters, security)</td><td>1</td></tr><tr><td>Student</td><td>0</td></tr><tr><td>Other</td><td>2</td></tr></table>	Clinical	21	Administrative and Clerical	4	Management	5	Professional, Scientific and Technical (ex scientist, lab techs, pharmacist, psychologist, radiographer, engineers, IT, and data professionals, etc)	8	Estates and Ancillary (ex maintenance, cleaning/housekeeping, porters, security)	1	Student	0	Other	2
Clinical	21															
Administrative and Clerical	4															
Management	5															
Professional, Scientific and Technical (ex scientist, lab techs, pharmacist, psychologist, radiographer, engineers, IT, and data professionals, etc)	8															
Estates and Ancillary (ex maintenance, cleaning/housekeeping, porters, security)	1															
Student	0															
Other	2															
2. How long have you worked in Falkland Islands Health & Social Services?	0-3 years 27% 4 – 10 years 29% 10+ years 44%	<table><tr><td>0 - 3 years</td><td>27%</td></tr><tr><td>4 - 10 years</td><td>29%</td></tr><tr><td>10+ years</td><td>44%</td></tr></table>	0 - 3 years	27%	4 - 10 years	29%	10+ years	44%								
0 - 3 years	27%															
4 - 10 years	29%															
10+ years	44%															
3. Do you interact directly with patients and members of the public as part of your job?	Yes, every day 71%, Yes, every week 15% Yes, every month 1% Rarely 10% Never 1%	<table><tr><td>Yes, every day</td><td>71%</td></tr><tr><td>Yes, every week</td><td>15%</td></tr><tr><td>Yes, every month</td><td>1%</td></tr><tr><td>Rarely</td><td>10%</td></tr><tr><td>Never</td><td>1%</td></tr></table>	Yes, every day	71%	Yes, every week	15%	Yes, every month	1%	Rarely	10%	Never	1%				
Yes, every day	71%															
Yes, every week	15%															
Yes, every month	1%															
Rarely	10%															
Never	1%															
4. Do you record (write down or capture) what patients and service users tell or show you? (E.g. On paper, a computer, a phone, a camera?)	Yes, every day 61% Yes, every week 15% Yes, every month 5% Rarely 7% Never 12%	<table><tr><td>Yes, every day</td><td>61%</td></tr><tr><td>Yes, every week</td><td>15%</td></tr><tr><td>Yes, every month</td><td>5%</td></tr><tr><td>Rarely</td><td>7%</td></tr><tr><td>Never</td><td>12%</td></tr></table>	Yes, every day	61%	Yes, every week	15%	Yes, every month	5%	Rarely	7%	Never	12%				
Yes, every day	61%															
Yes, every week	15%															
Yes, every month	5%															
Rarely	7%															
Never	12%															

5. Have you completed any confidentiality-related training within the last 24 months?	Yes 95% No 5%	- Yes - No - Can't remember 
6. Do you understand the Code of Confidentiality and your responsibilities under it?	Yes, fully 98% Yes, partly 2% No 0%	- Yes, fully - Yes, partly - No 
7. Do you know how to raise concerns about confidentiality of patient data?	Yes 100% No 0% Unsure 0%	- Yes - No - Unsure 
8. How confident do you feel that you understand how to keep patient information safe?	Very confident 83% Somewhat confident 17% Neutral 0% Not very confident 0% Not at all confident 0%	- Very confident - Somewhat confident - Neutral - Not very confident - Not at all confident 
9. Do you have access to enough patient information to do your job?	All of the time 49% Sometimes 29% I don't need to access patient information 22%	- All of the time - Sometimes - Rarely - Never - I don't need to access patient information 

10. Do you ever have access to more patient information than you need?	Yes 7% No 78% Unsure 15%	
11. Have you ever talked to a patient or service user about what happens to the information they tell you?	Yes 63% No 32% Unsure 5%	
12. What is the biggest risk to patient confidentiality at KEMH? (Select a category and describe)	People 66% Processes 1% Technology 12% Other e.g. environment 20%	
13. Briefly describe risk: 41 responses. Most confidentiality breaches stem from people, but the physical environment, small community context, outdated systems, and weak processes all increase the likelihood and impact of human error.		
14. Have you identified a concern about patient confidentiality in the last 12 months?	Yes, and reported it 37% Yes, but did not report it 7% No 56%	
15. Do you believe the organisation promotes a culture for self-reporting when things go wrong?	Yes 68% No 15% Unsure 17%	
16. Since you first started in your role, how has the culture around self-reporting changed?	Improved 51% Got worse 2% Stayed the same 27% Unsure 20%	

17. Have you ever witnessed or been involved as a member of staff in an information governance (IG) incident or confidentiality breach?	Yes 49% No 41% Unsure 10%	
18. If yes, please describe briefly but do not include any names. 20 responses outlined the main risks come from human error (misaddressed emails, wrong records, unlocked PCs), misidentification, and weak controls around system access & patient images. Physical and digital processes often fail at basic identity checks, leading to preventable breaches.		
19. To your knowledge, have there been any confidentiality breaches?	Yes, in the last 12 months 32% Yes, more than one year ago but after 2022 10% No 10% Don't know 22%	
20. Does the Electronic Patient Record (EMIS PCS) system support secure and efficient data handling?	Yes 34% No 27% Unsure 39%	
21. What improvements would you suggest for systems or environment to strengthen confidentiality? 41 responses. Staff are calling for modern digital systems, improved physical spaces, stronger access controls, and a more robust confidentiality culture supported by practical training and clearer governance.		
22. Would you enable colleagues to access EMIS or other systems using your log in/password? Select all applicable reasons below.	Never 27 For rapid access in an emergency 14 If a colleague was locked out of the system 1 Other 4	

23. If you selected 'other' please explain:	9 responses. Respondents indicated that they do not share access or use EMIS on behalf of others, with several stating they do not have EMIS access at all. Where exceptions were mentioned, these were limited, situational, and provided clinical justification, such as: supervised or joint working, out-of-hours emergency, or data access only when necessary	
24. Do you feel you have enough guidance and resources on IG and confidentiality?	Yes 80% No 12% Unsure 7%	A donut chart with three segments: a large blue segment for 'Yes' (80%), a smaller pink segment for 'No' (12%), and a very small green segment for 'Unsure' (7%). A legend to the left of the chart identifies the colors: blue for Yes, pink for No, and green for Unsure.
25. Would you like additional training or refreshers? (Select all that apply)	Data protection 14 Caldicott principles 12 Secure record handling 10 Incident reporting 11 Cyber risk 12 Artificial Intelligence 24 Other 5	A horizontal bar chart with seven bars of different colors. The x-axis is labeled from 0 to 25 in increments of 5. The bars represent the following categories and counts: Data protection (blue, 14), Caldicott Principles (pink, 12), Secure record handling (teal, 10), Incident reporting (purple, 11), Cyber risk (green, 12), Artificial Intelligence (light blue, 24), and Other (orange, 5). A legend to the left of the chart identifies the colors for each category.
26. If other, please describe.		
4 responses. Respondents felt that training is already available and accessible, with acknowledgement that existing training provision is good. However, several comments highlighted areas for improvement, including regular auditing around IG practices, concerns around unclear policies around data transfer, uncertainty around WhatsApp for sharing patient information.		
27. Can you share any positive examples of information governance you've observed, and the services where they took place?		
41 Responses. Overall, responses demonstrate a strong awareness and routine application of confidentiality and IG principles across the organisation. Many respondents felt this is embedded in daily practice and reflected in staff behaviour, decision-making, and culture. For example, setting boundaries, consent, cross-agency, and overseas data sharing.		
28. What improvements would you suggest to strengthen confidentiality and information governance?		
41 responses. Overall, respondents identified training and awareness as the strongest positive example of information governance, noting that regular IG training, CPD, refreshers, and lectures have improved staff understanding of confidentiality responsibilities across services. Leadership and culture were also highlighted, with managers and senior clinicians leading by example and a growing emphasis on individual accountability and a no-blame culture. In some areas, improved IT systems, access controls, clearer desk policies, and more secure working environments were seen as supporting better governance, alongside clearer frameworks and reminders that help staff apply good practice day to day.		
29. Is there anything else you would like to share confidentially with the reviewers?		

25 responses. Overall, respondents described a highly emotionally charged and stressful environment arising from confidentiality breaches and the intense public scrutiny surrounding them, particularly in the context of a small community. While many acknowledged the need for accountability, learning, and improved practice, there was a strong sense that the situation has at times felt like a witch hunt, negatively affecting staff morale, wellbeing, and confidence. Staff reported anxiety, fear of sharing information even when appropriate, damaged trust between colleagues, and concerns that this climate may compromise patient care. Some also highlighted specific breaches of confidentiality affecting staff themselves, calls for cultural change to address gossip, inconsistent training uptake, and gaps in systems and leadership. Despite this, several respondents felt the review process was positive, offering an opportunity for reflection, improvement, and the hope of drawing a line under past events so both staff and patients can recover and move forward