

Falkland Islands Government
Health and Social Services Directorate



Code of Confidentiality Policy

Author: Director of Health and Social Services

Issue Date: March 2025

Version No: V6.1 Status:

Draft – for final approval

Review date: July 2027

Amendment History

Version	Status	Summary of changes	Date of issue
V1.0	Final		June 2007
V2.0	Final	Revised and updated, contents list added.	July 2014
V3.0	Final	Additional section added to Annex 3	Oct 2014
V4.0	Final	Revised & updated to include additional revised Caldicott Principles and inclusion of Capacity in relation to Mental Capacity Act 2005 Approved by SMT July 2019 Approved by HMSC August 2019	July/August 2019
V5.0	Final	Revised and updated to include update on Caldicott principles. Approved by SMT July 2022	July 2022
V6.0	Final	Annex 4 added to the policy	July 2024
V6.1	Revision Feb 2025	Section 1.4 c – Page 13: Removal of ‘faxes’ Section 4 – Definitions - Page 5: 4.3 Revised by Adult Social Worker to include up-date on ‘Mental Capacity’ and DoL draft Ordinance Section 9 – Page 10: List of References reviewed and revised. ‘Vulnerable Adults’ changed to Adults at risk throughout the document Removal of reference to Information Sharing Document 2017	
V6.1	Final	Changes agreed and approved by SMT members	March 2025

<u>Contents</u>	<u>Page</u>
Introduction	3
1. Aims	3
2. Principles	3
3. Scope	4
4. Definitions	5
5. Responsibilities	6
6. Disclosing and using confidential information	7
7. Disclosure in the public interest	8
8. Breaches of confidentiality	9
9. References	10
10. Auditable standards	10
Annex 1 The Confidentiality Model	11
1. Protect Patient/client information	11
1.1. Recognising that confidentiality is an obligation for all staff, External contractors and volunteers	11
1.2. Keeping patient/client information private	11
1.3. Keeping patient/client information physically and electronically secure	12
1.4. Disclosing information with appropriate care	13
2. Inform Patient/clients effectively – No Surprises	13
2.1. Let patient/clients know what information you wish to record or that you are accessing their record	14
2.2. Make clear to patients when information is or may be disclosed to others	14
2.3. Check that patients are aware of the choices available in respect of how their information may be used or shared	14
2.4. Check that patients have no concerns about how their information is used	14
2.5. Respect the right of patients to have access to their health records	15
3. Offer and Respect Individuals' Choices	15
4. Improve Wherever Possible	15
Annex 2 Legal considerations	16
Annex 3 Guides to Confidentiality Decisions in Practice	18
Annex 4 Suspected Data/Breach of Confidentiality	24
Code of Confidentiality declaration document	26

Introduction

The Falkland Islands Health and Social Services Directorate is committed to the delivery of a confidential service.

Patients, clients and other service users entrust us with, or allow us to gather, sensitive information about their health and other matters as part of seeking treatment. They do so with the legitimate expectation that staff will respect their privacy and act appropriately.

Confidentiality is a vital element of good care. A lack of trust may prevent people from seeking medical attention; may cause them to withhold important, sensitive details; or may cause a level of anxiety that impedes the therapeutic process.

It is essential that the Department provides, and is seen to provide, a confidential service to all our service users. This is particularly important in our small community, the size of which makes privacy difficult to attain.

This policy seeks to make explicit the behavior expected, and to ensure that everyone strives to meet these standards. Staff may be constrained from achieving standards where appropriate organisational systems are not in place, and existing systems and processes may also need to change and it is important that staff inform a member of the management team of any specific problems or barriers to confidentiality.

The code relates specifically to patient and client information. Confidentiality in regard to other types of information is covered by the FIG Management Code.

1. Aim

To provide a code of conduct for employees and contractors working for the Falkland Islands health and social services departments in relation to confidentiality of patient information.

Objectives:

1. To define confidentiality and confidential information – see Caldicott Principles below.
2. To make explicit the standards of conduct expected of health and social care staff
3. To describe the legal framework governing confidentiality in the Falkland Islands
4. To provide guidance on disclosure of information

2. Principles

Information that has been shared by the patient with the healthcare employee is privileged and confidential information. A patient's health records are made by the health service in order to support that patient's healthcare. This means that information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. The same principles apply to social services and information provided for the purposes of social care.

The principles underlying this document are modelled on the Caldicott Principles adopted by the National Health Service UK. They are:

CALDICOTT PRINCIPLES

1. Justify the purpose.

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

2. Use confidential information 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 confidential information.

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 confidential information should be on a strict need-to-know basis.

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 confidential information 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 can be as important for individual care as is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of patient supported by the policies of their employers, regulators and professional bodies.

8. Inform patients and service users about how their confidential 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.

(National Data Guardian for health and social care December 2020 www.gov.uk accessed 28 July 2022)

3. Scope

This policy document applies to all employees, including casual and bank staff, as well as volunteers and contractors working with the FIG Health and Social Services Directorate. It also applies to any employee or contractor of the Falkland Islands Government who is privy to patient information in the course of their duties.

Information can be held on a range of media including paper, hard disk, tape, radiology images, document images, video and photographs. This policy applies to the use of all attributable information from which an individual may be identified, both oral and recorded.

4. Definitions

The Oxford English Dictionary has the following definitions:

1. To confide: to tell someone about a secret or private matter while trusting them not to repeat it to others
2. Confidential: intended to be kept secret or private
3. Capacity: The FIG Mental Capacity in the Falkland Islands policy defines the following principles which have been adopted from the Mental Capacity Act 2005 (UK).
 - A person must be assumed to have capacity unless it is established that they lack capacity
 - A person is not to be treated as unable to make a decision unless all practicable steps to help them to do so have been taken without success
 - A person is not to be treated as unable to make a decision merely because they make an unwise decision
 - An act done, or decision made, under this policy, for or on behalf of a person who lacks capacity, must be done, or made, in their best interests
 - Before the act is done, or the decision is made, regard must be had as to whether the purpose for which it is needed can be as effectively achieved in a way that is less restrictive of the person's rights and freedom of action.

A person lacks capacity in relation to a matter if at the material time the person is unable to make a decision for themselves in relation to the matter because of an impairment of, or disturbance in the function of, the mind or brain.

3.1. It does not matter whether the impairment or disturbance is permanent or temporary.

3.2. A lack of capacity cannot be established merely by reference to:

- (a) a person's age or appearance;
- (b) a condition of the person, or an aspect of the person's behaviour, which might lead others to make unjustified assumptions about the person's capacity.

The Falkland Islands Mental Capacity and Deprivation of Liberty Ordinance (draft) will contain the necessary legal safeguards required to support people who lack mental capacity to make decisions.

What is confidential patient/client information?

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It –

- a. is a legal obligation that is derived from case law;
- b. is a requirement established within professional codes of conduct; and
- c. is included within FIG Health and Social Services employment contracts as a

specific requirement linked to disciplinary procedures.

- d. is not absolute where there are concerns that harm may come to an individual(s) and that level of harm overrides the breach of confidentiality, this is especially relevant to children, young people and those with increased vulnerability

Patient/Client Identifiable Information. Key identifiable information includes:

- Person's name, address, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients/clients;
- EPR (Electronic Patient Records) and X-ray or Social Service case numbers – however within the department these are a useful tool for emailing between staff so long as non-gender specific terminology is used;
- *Anything else that may be used to identify a service user directly or indirectly.* For example, unusual conditions/diseases, circumstances or drug treatments, or statistical analyses of very small numbers within a small population, may allow the identification of individuals.

Anonymised information. Information which does not identify an individual directly, and which cannot reasonably be used to determine identity. It requires the removal of name, address and *any other detail or combination of details* that might help identify the patient/client. Anonymised information is not confidential and can be used with relatively few constraints.

Caldicott Guardian. The Person appointed in an organisation to protect the confidentiality of patients and services users and enable appropriate information sharing. Presently this is the responsibility of the Chief Medical Officer (CMO) or a designated deputy.

Case Law. Law based on actual cases that have been before a court rather than drafted legislation

Explicit/Express Consent. A clear indication of preference or choice, freely given, usually either orally or in writing, after the available options and consequences have been made clear. **Implied consent** occurs when the behaviour of an informed patient/client signals their agreement.

Disclosure. The divulging or provision of access to data.

Healthcare Purposes These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

Information Sharing Protocols. Documented rules and procedures for the disclosure and use of patient/client information, that specifically relate to security, confidentiality and data destruction, between two or more organizations or agencies such as Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers in the Falkland Islands April 2017

Public Interest. Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.

Safeguarding. The overriding principle that the safety of and welfare of all and especially children and adults at risk is paramount

Social Care. Social care is the support provided for children or adults at risk, including those with disabilities. It excludes “pure” health care (hospitals) and community care (e.g. district nurses), but may include items such as support at home with daily living skills, family work, day care, family respite for people with social needs, etc. There is, therefore, no clear demarcation line between health and social care. This is particularly true in the case of the Falkland Islands where health and social care are part of the same directorate and overarching organisation (FIG).

5. Responsibilities

All staff, contractors and volunteers have a duty to:

- Treat all patient information in the strictest confidence
- Ensure that all information relating to patients is only used for the purposes for which it was given

Staff, contractors and volunteers must:

- be aware of their personal responsibility and abide by this code
- not access any record for which they do not have a proper reason in the course of their duties
- not access records for their personal interest

Managers must:

- Ensure that staff, students, agency staff, temporary/casual staff and volunteers are aware of the code of confidentiality and sign declarations of confidentiality on starting work in the department
- Make staff aware of how and when to seek advice on matters of confidentiality and disclosure

Ensure that contract staff are bound by the same code of confidentiality as employed staff in all contracts with third parties.

6. Disclosing and Using Confidential Information

The primary use of health and social information is for the delivery of personal care and treatment. As a general rule, staff should not disclose or use any information provided in confidence in a form that might identify the patient/client without the patient/client's consent. Patient/clients generally have the right to object to the use and disclosure of confidential information that identifies them, and staff should make them aware of this right.

However, information is needed, and may be disclosed, for other health and social care purposes:

- safeguarding people especially including children, young people and adults at risk
- assuring and monitoring the quality of care and treatment e.g. through audit
- monitoring and protecting public health
- coordinating care with other agencies e.g. health/social services, education
- effective management e.g. service planning, contracting, financial/probity audits
- education and training
- statistical analysis
- the broader public interest including the prevention and detection of serious crime and as ordered by the courts

Further details on information disclosure and sharing can be found in the Annexes to this document.

Patient/Client Consent to Disclosing

Explicit consent is not usually required for information disclosures needed to provide healthcare e.g. sharing of information with other members of the clinical team. Even so, it is good practice to check that patient/clients understand and are content with what may happen. For example, patients may not be aware of the extent to which information is available to all members of the clinical team via EPR. Staff should take into consideration whether the patient has capacity to understand as per section 4.

However, staff must also inform patient/clients if their decisions about disclosure have implications for the provision of their care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition, medical history, assessment and plan of care as a minimum.

There are situations where consent cannot be obtained for the use or disclosure of patient/client identifiable information, yet the public good of this use outweighs issues of privacy. This includes the use of patient/client identifiable information to support important healthcare related work such as clinical audit and record validation, carried out by members of the wider healthcare team.

7. Disclosures in the Public Interest

There are exceptions to the duty of confidence that may make the use or disclosure of confidential information appropriate. UK case law has established that confidentiality can be breached where there is an overriding public interest. This would carry weight in the Falkland Islands.

Disclosure of personal information is permitted where a member of staff judges, in an individual case, that disclosure will:

- Prevent or support detection, investigation and prosecution of serious crime
- or**
- Prevent abuse or serious harm to others (including the patient/client concerned)
- and**
- that the public good achieved by disclosure would outweigh
- both** the obligation of confidentiality to the individual concerned
- and** the broader public interest in the provision of a confidential service

All such decisions should be referred to the Director of Health and Social Services and/or Chief Medical Officer or their deputies as soon as possible. Each case will be considered carefully but it may sometimes be difficult to make a judgement. The advice of the Attorney General or other specialist (e.g. a professional, regulatory or indemnifying body) may be needed, or it may be necessary to await/seek a court order.

As far as possible, a discussion about disclosure should take place with the individual concerned and their consent sought. Where consent is not given, the individual should be told of any decision to disclose against his/her wishes. This will not be possible in certain circumstances, e.g. where a violent response is likely or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

The senior staff member who authorises the disclosure must make a clear record of the circumstances and rationale. Disclosures in the public interest should be proportionate and limited to relevant details. It may be necessary to justify such disclosures later to the courts or to professional regulatory bodies and a clear record of the decision-making process and the advice sought is in the interest of both staff and FIG.

NB It is important not to confuse “the public interest” with what is “of interest” to the public

Serious Crime and National Security

The definition of serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to state security or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would not generally warrant breach of confidence.

Risk of Harm

Disclosures to prevent serious harm or abuse also warrant breach of confidence. The risk of child abuse or neglect, assault, a traffic accident or the spread of an infectious disease are perhaps the most common that staff may face. However, consideration of harm should also inform decisions about disclosure in relation to crime. Serious fraud or theft involving health service/FIG resources would be likely to harm individuals needing treatment. It is also important to consider the impact of harm or neglect from the point of view of the victim(s) and to take account of the psychological as well as physical damage. For example, the psychological impact of child abuse, domestic abuse or neglect may harm children who know of it in addition to the child/family member concerned.

8. Breaches of Confidentiality

Staff are strongly encouraged to report any breaches of confidentiality, either deliberate or inadvertent, verbally, in the first instance, to their immediate line manager. This should be followed up by recording the incident formally using the Q- Pulse Incident Reporting Module and Caldicott Guardian.

Where members of staff ‘self-report’ incidents during which they have compromised the principles of the Code, a ‘no blame’ approach will normally be adopted. In these circumstances, disciplinary action will not normally follow.

However, where there is a deliberate or repeated accidental, unauthorised disclosure of any confidential information, disciplinary action may result against the individual(s) concerned.

Deliberate breaches, such as gossip, will be treated as gross misconduct, and may result in dismissal.

Any reports or disciplinary action will take account of the confidential, and possibly sensitive, nature of the information and will make sure that, in dealing with it, no further breaches of confidentiality take place.

9. **References**

<https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf>

<https://www.gmc-uk.org/professional-standards/the-professional-standards/confidentiality>

https://assets.publishing.service.gov.uk/media/5a7c13f0ed915d210ade16fb/Confidentiality_-_NHS_Code_of_Practice.pdf

10. **Auditable standards:**

An annual audit in January will identify staff that:

100% staff will have signed code of confidentiality form (as at end of policy)

Of a cross section of staff 90%, will know who the Caldicott Guardian is

80% of staff will have undertaken mandatory training about information governance

ANNEX 1

The Confidentiality Model

The model outlines the requirements that must be met in order to provide patient/clients with a confidential service. The four elements are:

1. PROTECT	look after the patient/client's information
2. INVOLVE and INFORM	ensure that patient/clients are aware of how their information is used;
3. PROVIDE CHOICE	allow patient/clients to decide whether their information can be disclosed or used in particular ways.
4. IMPROVE	constantly review confidentiality and seek ways to improve

1. Protect Patient/client Information

Patient/clients' health information and their interests must be protected through a number of measures:

1.1. Recognising that confidentiality is an obligation for all staff, external contractors, and volunteers.

- Breach of confidence, inappropriate use of health records or abuse of computer systems may lead to disciplinary measures. Staff should ensure that they are aware of the requirements and standards of behaviour that apply.
- Voluntary staff who are not employees, and students, are also under obligations of confidentiality, and must sign an agreement indicating their understanding when helping within health and social services.

1.2. Keeping patient/client information private

This includes:

- Not gossiping. This is clearly an improper use of confidential information. Even revealing that a patient has been in the hospital building is a breach of confidentiality.
- Not accessing patient's records without good reason. It is unacceptable to access a patient's record or to read patient notes, unless the information is needed for the patient's treatment or care, or the administration of that care.
- Taking care when discussing cases in public places. It may be relevant to discuss cases with colleagues (to gain advice or support, or to share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the patient/client, although it is recognised that it may be difficult to avoid the other party identifying the patient.
- Being aware of the dangers of breaching confidentiality inadvertently by the misuse of patient/client identifiable information including e.g. the circumstances of an accident.

1.3. Keeping patient/client information physically and electronically secure

Staff should not leave portable computers, electronic storage media, medical notes, files or other patient/client-related documents in unattended or easily accessible areas. Ideally, staff should store all files and portable equipment under lock and key when not in use. Staff should not normally take patient/client records from the workplace premises, but where this is unavoidable; procedures for safeguarding the information should be agreed in advance with the appropriate member of the Senior Management Team.

For all types of records, staff working in offices where records may be seen must:

- Shut/lock doors and cabinets as required.
- Query the status of anyone in a restricted (i.e. non-patient) area.
- Report to your manager if anything suspicious or worrying is noted.
- Not tell unauthorised staff how security systems operate.
- Not breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked, if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the clinical area or office, arranged so that they can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Destroyed using a secure means, e.g. shredding, where appropriate.

With electronic records, staff must:

- Always log out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff need to access records, appropriate access should be organised for them.
- Not reveal passwords to others or hide them where others can find them.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children's or pet's names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver to prevent casual viewing by others.

1.4. Disclosing information with appropriate care

- a) Follow any established information sharing protocols.

Information sharing protocols are in place for use between the hospital and social services team, and for wider use amongst other appropriate agencies. These set out the standards and procedures that should apply when disclosing confidential patient/client information with other departments and organisations. Staff must work within these protocols and within the spirit of this code of practice where they are absent. Awareness of the 'need to know' principle will guide staff where there is no written guidance.

- b) Identify enquirers, so that information is only shared with the right people.

Staff should check the identity of callers by telephone. Do not rely on recognising the caller's voice. If you do not know them or are unsure, check the identity of people presenting in person seeking confidential information.

Check that they have a legitimate right to have access the information requested. Even close relatives may not have the patient/client's consent for information to be shared.

There is a remote possibility that someone tries to gain information improperly by impersonation. If in doubt, seek official identification or check identity by calling the person back (using an independent source for the phone number).

- c) Ensure that appropriate standards are applied for e-mails and surface mail

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be. If emailing patient/client information which may need to be added to the patient/client's record, send separate emails for each person. Email correspondence relating to patient/clients should ALWAYS be written in formal language. Use an identification number such as an EPR number as identification rather than a name as well as neutral language, such as they, rather than he or she.

- d) Share the **minimum necessary** to provide safe care or satisfy other purposes.

This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence.

2. Inform Patient/clients effectively – No Surprises

Patient/clients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support local clinical audit and other work to monitor the quality of care provided. Consider whether patient/clients would be surprised to learn that their information was being used in this way. In order to inform patient/clients properly, staff must:

2.1. Let patient/clients know what information you wish to record or that you are accessing their record

This may require a simple comment such as *'Let me note that on your record' or 'its ok for me to just check in your notes?'*. However, supporting documentation around this is being developed by the Information Governance Group.

2.2. Make clear to patients when information is or may be disclosed to others

- a) Patients may not know exactly how the hospital and related departments (e.g. Social Services, Police and Education) work – aspects that staff may take for granted. Staff must ensure that patients know when data is disclosed or used more widely e.g.:
 - i. *'All clinicians in the hospital are able to view your health records to understand your medical history and the tests we have arranged'; or*
 - ii. *'I am writing to the xx to let them know about the abdominal pains you are having'; or*
 - iii. *'I will tell Social Services about your care needs so that an assessment can be made'.*
- b) There are certain Ordinances that require disclosure such as the Finance and Audit Ordinance 1988. This gives legal right of access to all government records to auditors appointed by the Government. Whilst information will be anonymised or consent sought wherever practicable, this may not always be possible or desirable. However, government auditors are bound by an oath of secrecy that prevents them from inappropriately disclosing the information that they need to access. External audit firms and their professional staff are also bound by professional codes of conduct.

Court orders may also require a disclosure. The amount of information disclosed should always be proportionate to the actual need. Even though the patient cannot prevent this disclosure, they must normally be told that it is taking place or that it has already occurred if this is the case.

2.3. Check that patients are aware of the choices available in respect of how their information may be used or shared

Patients have the right to choose whether the information they have provided in confidence can be used or shared beyond what they understood to be the case when they provided it. See Paragraph 7 of the Code and Annex 3 for exceptions.

2.4. Check that patients have no concerns about how their information is used

- a. It is important that patients feel free to raise any queries or concerns. In most circumstances it may require no more than a follow-up question to the above
- b. In other cases, if the information being recorded is particularly sensitive to the patient concerned, staff should be explicit about what is being recorded, and ask the patient directly if they are happy for that information to be shared.

It is much better for patients if their concerns can be addressed immediately, but, if staff cannot answer the questions properly, they should refer the patient to an appropriate member of the Senior Management Team.

2.5. Respect the right of patients to have access to their health records

There is no data protection legislation in force in the Falkland Islands. Patients' rights to access their own health records are covered by the Access to Health Records Ordinance 1995.

3. Offer and Respect Individuals' Choices

Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another: just because something does not appear to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances.

Patients have the right to choose whether or not to accept a form of care and the information disclosure needed to provide that care. Whilst it is necessary to disclose information about a patient to those staff who are providing or auditing care, it is important to ensure that those who see information have a genuine need to know.

Staff must:

- a. ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care;
- b. respect patients' decisions to restrict the disclosure or use of information, except where exceptional circumstances apply;
- c. communicate effectively with patients to ensure they understand clearly the implications of disclosing or not disclosing. Where patients insist on restricting how information may be used or shared in ways that compromise the health service's ability to provide them with high quality care, this should be documented within the patient's record. Staff should make clear to the patient that they can change their mind later.

If you cannot respect a patient's wishes on the use of personal health information, seek the advice of your line manager.

4. Improve Wherever Possible

If staff identify breaches, or risk of breaches of confidentiality, or abuse of patient data, then they must report them to their manager. The management team will support staff who report such matters. Staff may also choose to contact their professional or indemnifying bodies for guidance. Such breaches will be logged under the incident reporting procedure so that any common themes or trends can be identified and any lessons can be learned.

We are aware of the limitations of our current Electronic Patient Record system (EMIS) and are actively seeking an alternative to meet our needs, but to date, technical barriers are preventing this.

However, we have made considerable changes to working practices and processes following recent data breaches.

ANNEX 2

Legal Considerations

The disclosure and use of confidential patient information needs to be both lawful and ethical. The law and ethics are largely in step, but the law provides a minimum standard that does not always reflect the appropriate ethical standards that the government and the professional regulatory bodies require. For example, the Health Department and the Attorney General's Department are in agreement that, whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for continuing to apply confidentiality obligations, as outlined in this document. Further, where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

There are a range of statutory provisions that limit or prohibit the use and disclosure of information and, similarly, a range of statutory provisions that require information to be used or disclosed. Generally, there are four main areas of law that constrain the use and disclosure of confidential personal health information. These are described briefly below.

Common Law of Confidentiality

This is not codified in an Ordinance but built up from case law where practice has been established by individual judgements. There is no case law of the Falkland Islands Courts with regard to confidentiality. However, case law of the English courts, although not binding, is of persuasive authority, and for example a decision of the House of Lords would be greatly persuasive.

The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. However, judgments of the English courts have established that confidentiality can be breached 'in the public interest', on a case-by-case consideration of exceptional circumstances. Confidentiality can be overridden or set aside by legislation. Guidance should be sought from the FIG Sharing Information Guidance April 2017.

The Falkland Islands Constitution

In the Islands, we have the Constitution made by Order in Council in 2008, which guarantees the protection of a number of fundamental rights and freedoms. The protections of the Constitution specifically underscore in general terms the protection for family life, personal privacy, and the privacy of home and other property.

Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "*ultra vires*", i.e. beyond its lawful powers. It is also necessary that the power be exercised for the purpose for which it was created or be "reasonably incidental" to the defined purpose.

The principle here is that unless legislation explicitly requires that confidential patient

information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place e.g. by obtaining explicit patient consent.

Access to Health Records Ordinance 1995

This ordinance sets out the rights of patients to access their own health records.

UK Legislation Not Applying in the Falkland Islands

It is important to note that some UK legislation does not apply in the Falkland Islands. The following are not within our legislative or regulatory framework:

- Data Protection Act 2018
- Section 60 Health and Social Care Act 2001
- The Health Service (Control of Patient Information) Regulations 2002
- Crime and Disorder Act 1998
- General Data Protection Regulations (GDPR) 2016

ANNEX 3

Guides to Confidentiality Decisions in Practice

To Health Staff involved in the provision of Healthcare	Where information has to be shared widely to provide healthcare, try to ensure that patients are effectively informed of the extent of information sharing.
To social workers involved in the provision of Healthcare	The test of what would satisfy the requirement to inform effectively should be more demanding than where disclosure is limited to health staff as the breadth of the information disclosure is not as obvious to patients and their consent cannot be assumed. Disclosure may lead to confidential information being held outside the hospital. Patients need to be made aware of this and the social service team needs to be aware that holding health records imposes particular duties and obligations. The social services team has introduced a consent form to enable the two-way sharing of information with health service colleagues. Where consent has been given, this will be noted on the patient's Electronic Patient Record.
To clinical auditors	The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services, is an essential component of modern healthcare provision. Every effort should be made to ensure that patients are aware that audit takes place and that it is essential if the quality of care they receive is to be monitored and improved. However, patient identifiable information for this purpose can be used without explicit consent
To parents, i.e. those with parental responsibility for parents and guardians	Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults . Children under 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected. The key issue here is the 'competence' of the child. If the child is competent then their consent is required to disclose and use information. Staff should encourage children to involve parents, particularly where significant decisions need to be made, but should respect the choice made. However, where a child has refused to consent to treatment for a life-threatening condition, staff should inform parents and seek their consent (consent for treatment purposes may be given by parents even where a child objects). A parent always retains parental responsibility for their child. For children in Stanley House, parents may transfer part of their responsibility to the house parents, but the house parents' responsibility is limited to doing what is reasonable in the circumstances to safeguard the child's welfare. This would cover, for example, the situation where urgent medical attention is required in circumstances where it is impossible or impracticable for the parents to be contacted. In practice, the parents of a child found not to be Gillick competent should always be informed of any medical advice or treatment. It is advised, however, that any advice or treatment given whilst the child is at Stanley House School Hostel which may have a bearing on their welfare whilst at the hostel should also be disclosed to the relevant House Parent.
To those under 18 years	If you are a young person aged 16 or 17 you are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults. If you are under 16 but over 13 the health professional you are seeing may be able to assess your capacity and

	<p>understanding to take decisions about your own treatment. If the health professional does feel comfortable that you can do this then you are entitled to decide whether personal information may be passed on and have your confidence respected.</p> <p>The health professional will have to judge you have sufficient understanding and maturity to enable you to understand fully what is being proposed and are capable of expressing your own wishes. You must be able to understand the advice being given and must indicate that you cannot be persuaded to involve your parents and that you would be likely to continue with your health risks, i.e. continue to have sexual intercourse with or without advice or treatment. The health professional must be sure that if you do not receive the advice, i.e. contraceptive advice or treatment then your physical or mental health, or both, will suffer and your best interests require us to give you the advice, i.e. contraceptive advice or treatment, or both, without parental consent. Under these circumstances consent is required to disclose and use information. Your parents, however, still have responsibility for you and staff will always encourage you, and will be able to help you, to share information with them. This is because parents in general are best able to support and care for you, even when it is challenging for them. Where any member of staff is concerned about your safety, they have a duty to you to share information to keep you safe.</p> <p>If you are under 13 health professionals have a responsibility to respect you and the information you are providing and would expect to have parental or carer involvement in all decisions.</p>
To carers without parental responsibility	<p>Carers often provide valuable healthcare and, subject to complying with the best practice outlined, every effort should be made to support and facilitate their work. Only information essential to a patient's care should be disclosed and patients should be made aware that this is the case. However, the explicit consent of a competent patient is needed before disclosing information to a carer. The best interests of a patient who is not competent to consent may warrant disclosure.</p>
To Members of Legislative Assembly (MLAs), and to staff/managers in other FIG departments requiring information for healthcare purposes	<p>Government departments require a range of information to carry out their functions. There needs to be a means to permit desired information disclosure and tests of appropriateness and necessity must be satisfied.</p> <p>The use of anonymised data is preferable for management purposes outside the health service but within FIG (e.g. to inform Executive Council policy decisions or to seek advice/decisions on such matters as medical entitlement, evacuation or repatriation etc.) but this is not always practicable.)</p> <p>However, the use of confidential (patient identifiable) information to support these activities may be appropriate and necessary, and, in certain individual cases, it may not be possible to protect the patient's anonymity. Care should always be taken to determine the minimum requirements. Explicit consent is required unless there is (rarely) a robust public interest justification.</p> <p>Treasury staff will necessarily have access to some patient information in order process payment vouchers for e.g. overseas treatment-related expenses. Treasury staff must take an oath or affirmation of secrecy which obliges them not to disclose any information which comes to them in the course of their duties except in accordance with law. The Finance and Audit Ordinance entitles the Financial Secretary to access all documents and records relating to public monies; and to delegate that power of access.</p>
To researchers	<p>The use of anonymised data is preferable for research purposes. In some cases, where it is impossible to provide an anonymised data set for researchers, the use of identifiable patient information to support research may be</p>

	necessary but requires explicit patient consent.
To Occupational Health Professionals	Staff may be referred to the occupational health department, e.g. as a result of sickness absence or a perceived failure to meet work targets. This could in turn require disclosure of patient information. Explicit consent should be obtained before disclosing. It is particularly important that managers who have access to the EPR system or other information gained in the course of their work (e.g. organisation of an aeromedical evacuation) do not abuse this access or disclose such information without the explicit consent of the individual concerned.
To flight booking agents	Patients should be made aware that when a flight is booked in their name by the hospital, the booking agent will be aware that the purpose of the flight is medical. Such agents are not subject to this code of confidentiality but they are asked to respect it when dealing with patients' travel arrangements. They should also be aware that, if they do make information public, they could be subject to a civil action for damages by the patient and may have to justify their actions in court.
To insurance companies	In order to secure payment for treatment and care of non-entitled patients, confidential information about the patient's condition and treatment may have to be provided to an insurance company. Provision of such information is usually in the best interests of the patient. Nonetheless, the patient must be informed that this information will be released and, wherever practicable, the patient's consent should be obtained. Only information that is pertinent to the costs of the current episode of care should be passed on.
To shipping agents	<p>Foreign fishermen and other visitors deserve the same level of confidentiality as other patients. Fishing/shipping agents acting on behalf of a patient/ship often require confidential information regarding the patient's diagnosis and doctor's recommendations for their treatment in order to communicate these with the insurance company. It should be born in mind that it is often in the patient's best interests to obtain the consent of the insurance company to fund treatment, without which the patient may not receive optimum treatment. The patient should be informed that this information is to be released and the patient should be informed that this information will be released via the agent, and, wherever practical, their consent should be obtained. Only information that is pertinent to the costs of the current episode of care should be passed on.</p> <p>Where the agent is also acting as an interpreter/ translator, it may be difficult for the clinician to be sure that informed consent has been obtained. In providing information to the agent, clinicians need to balance the need for confidentiality against the practicalities of/need for providing treatment and getting the patient home. The agent must only use the information provided for the purpose for which it has been obtained. Professionals should remind agents and translators of the need to maintain confidentiality about information provided to them.</p> <p>As non-FIG employees, agents are not subject to this code but they should be asked to respect it when dealing with health matters. They will need to be aware that if they breach confidentiality, they could be subject to a civil action for damages by the patient concerned and may have to justify their actions in court.</p>
To interpreters and translators	Interpreters and translators will, of necessity, receive confidential information in the course of their duties. Whilst working on behalf of patients in the care of the FIG health service, they will be expected to maintain the same level of confidentiality as other members of the healthcare team. Breach of confidentiality may result in an action by the patient for civil damages.

<p>To clergy</p>	<p>Spiritual care cannot be practicably provided without access to some confidential patient information and this form of care is strongly desired by a proportion of patients. It therefore meets the tests of necessity and appropriateness. However, the explicit consent of patients is required before confidential information is disclosed to members of the clergy.</p> <p>Where a patient is not competent to consent to disclosure, e.g. due to unconsciousness, the decision rests with those responsible for the provision of care acting in the best interests of the patient. The views of family members about what the patient would have wanted should be given considerable weight in these circumstances.</p>
<p>To bodies with statutory investigative powers</p>	<p>The Finance and Audit Ordinance 1988 gives auditors appointed by Government (both internal and external) powers to access all records held by government officers, including health records. It is for auditors to decide what level of information is necessary for them to fulfil their functions, e.g. a complete record containing patient-identifiable information, selected parts or just anonymised information. Wherever possible and practicable, the use of anonymised data is preferable but it may be necessary for patient-identifiable information to be provided. If staff have concerns about the level of information requested, they should seek and document the reasons it is needed. Patients should be informed that disclosure has been required.</p> <p>Unlike in the UK, GMC assessors have no right of access to confidential patient records without explicit patient consent or a court order</p>
<p>To social workers in child protection cases</p>	<p>The FIG Safeguarding Policy covers issues of confidentiality in detail and includes specific guidance and procedures for different professional groups.</p> <p>The law permits professionals and agencies to <i>disclose without consent confidential information necessary to safeguard a child or children</i>. Professionals in the Falkland Islands will be concerned about the need to balance their duty to protect children from harm and their general duty towards their patient or service user, particularly where they are involved in caring for, or supporting, more than one family member - the abused child, siblings and an alleged abuser, for example. Professionals must remember that the <i>needs of the child must come first</i>. The General Medical Council has confirmed that its guidance on the disclosure of information which may assist in the prevention or detection of abuse, applies both to information about third parties (e.g. adults who may pose a risk of harm to a child) and about children who may be the subject of abuse. Nurses, Midwives and Health Visitors will wish to have regard to the guidelines of the Nursing and Midwifery Council. These authorise the disclosure of information without the consent of the patient or client when the disclosure can be justified in the public interest, usually where disclosure is essential to protect the patient or client or someone else from significant harm. Registrants are required to act at all times in accordance with national and local policies where there is an issue of child protection.</p> <p>If an allegation is made directly by a child you must explain, subject to the child's age and understanding, in a way that they can understand, that you have a duty to pass the information to the Social Work Department and or Police. It is important that you clearly state that you are required to report a child safeguarding concern. Do not offer confidentiality, reassure them that it is reasonable to make the allegation and of your interest in their safety.</p> <p>All professionals have a duty to inform the key worker of significant events relevant to any child on the child protection register.</p>

To the police	<p>Whilst the police have no general right of access to health records, there are a number of UK statutes which require or permit disclosure to them. They have the effect of making disclosure a legitimate function in the circumstances they cover although, in reality, they are unlikely to be relevant in the Falkland Islands context. In the absence of a requirement to disclose there must be either explicit patient consent or a robust public interest justification. What is or is not in the public interest is ultimately decided by the Courts.</p> <p>Where disclosure is justified it should be limited to the minimum necessary to meet the need and patients should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk. See definition of “serious crime.”</p>
To the courts, including coroner’s court, Commissions of Inquiry	<p>The courts and persons appointed to hold inquiries have legal powers to require disclosure of confidential patient information. Care needs to be taken to limit disclosure strictly in terms of the relevant order, the precise information requested to the specified bodies and no others. It is permitted to make ethical objections known to a judge or presiding officer, but unless the order is changed compliance is necessary.</p> <p>A Commission of Inquiry, established under the Ordinance of the same name, has the powers of the Supreme Court to call for documents whilst conducting an inquiry into a matter of public importance.</p>
To FIG Complaints Manager (outside health services)	<p>It is unlikely to be practicable for a manager to investigate a complaint without access to relevant parts of the complainant’s medical record, and anonymisation is not practicable. The use of identifiable information is therefore necessary and appropriate. However, the explicit consent of the complainant, and any other patients whose records may need to be reviewed, is required prior to disclosure. It may be necessary to explain to a complainant that their complaint cannot be progressed if they refuse to authorise disclosure.</p>
To non-statutory investigations e.g. Whistle-blowing Inquiries, Disciplinary Investigations/ Hearings	<p>If an investigation is appropriately authorised, disclosure will meet tests of necessity and appropriateness. The minimum necessary information should be disclosed. There is a balance to be drawn between ensuring that a patient has understood and properly consented to a disclosure of information and needlessly obstructing an investigation. Careful consideration of any written authorisation and prompt action are key, e.g. where an MLA states, in writing, that s/he has a patient’s consent for disclosure this may be accepted without further resort to the patient.</p>
To the media	<p>Under normal circumstances there is no basis for disclosure of confidential and identifiable information to the media. There will be occasions however when health staff are asked for information about individual patients. In these circumstances the most senior manager will be involved at an early stage linked with the FIG public relations and media department; Examples include:</p> <ul style="list-style-type: none"> • Requests for updates on the condition of particular patients, e.g. celebrities; • In distressing circumstances, e.g. following a fire or road traffic accident; • In circumstances where a patient or a patient’s relatives are complaining publicly about the treatment and care provided. <p>Where practicable, the explicit consent of the individual patient(s) concerned should be sought prior to disclosing any information about their care and treatment, including their presence in a hospital or other institution. Where consent cannot be obtained or is withheld, disclosure may still be justified in the “exceptional” public interest. In distressing circumstances, care should be taken to avoid breaching the confidentiality of patients whilst dealing sympathetically with requests for information. Where a patient is not competent to make a decision about disclosure, the views of family members should be sought and decisions made in the patient’s best interests.</p>

	<p>Where information is already in the public domain, placed there by individuals or by other agencies such as the police, consent is not required for confirmation or a simple statement that the information is incorrect. Where additional information is to be disclosed, e.g. to correct statements made to the media, patient consent should be sought but where it is withheld or cannot be obtained disclosure without consent may still be justified in the public interest. The patients concerned and/or their representatives should be advised of any forthcoming statement and the reasons for it. There is a strong public interest in sustaining the reputation of the health service as a secure and confidential service but there is a competing interest in ensuring that the reputations of health staff and the health service is not unfairly and publicly maligned. Disclosures need to be justified on a case by case basis and must be limited to the minimum necessary in the circumstances. In some circumstances a “dignified silence” in the face of media enquiry, may be the best approach for the health service to take, depending on the nature of the case involved.</p>
To Solicitors	<p>Most contacts from solicitors are for subject access requests to medical records for compensation claims which may include:</p> <ul style="list-style-type: none"> • insurance claims against third parties e.g. following road traffic accidents (RTAs); and • work related claims e.g. for disability awards, early retirement etc. <p>There may also be requests for prosecution purposes in cases of, for example, drink driving, RTAs, GBH and murder enquiries etc.</p> <p>Ideally, disclosure should be limited to information relevant to the incident concerned. However, if disclosure of the full record is required this should be complied with as long as it is clear that the patient understands and has consented to full disclosure. On occasions, when clinicians or health organisations face legal challenges, solicitors acting for a client may require access to a third party’s record. In such cases, explicit consent should be sought from any person or persons to which it relates. However, if a patient refuses consent, disclosure may still be warranted in the public interest or where a Court Order to support disclosure without consent has been received. It may be possible for a solicitor to make a public interest argument but this would be difficult to judge and best left to the Courts to decide. In all cases a patient should be notified of the disclosure.</p> <p>Where the health service faces a legal challenge, the advice of the AG’s Department should be sought immediately and any disclosure discussed with the AG in advance.</p>

Annex 4

Suspected Data/ Confidentiality Breach

When dealing with person- identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual/professional obligations and undertake to abide by the Health and Social Services Code of Confidentiality Policy.

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential Information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of Confidentiality, and, if upheld, will be subject to FIG disciplinary process and **may face dismissal or criminal prosecution**.

Initial Internal Investigation

Suspected Breach.

Line Manager/ Head of Service (HoS) to investigate – Inform HM, CMO & HGM

HGM may be required to conduct an initial Audit and remove access to EPR system whilst investigation is in progress

If there is a suspected breach within the Social Service's Azeus system, then the Head of Social Services will need to be notified.

An initial investigation will be conducted to identify if a breach has occurred.

During this investigation period, a non-blameworthy suspension may be put in place to protect the individual concerned and allow time to investigate thoroughly the suspected breach

Breach NOT upheld

Line Manager/HoS to consider additional training / supervision or other supportive actions. It may also be appropriate to give an informal 'Oral Warning' which is documented in the individuals 'P/file'.

Managers should clearly communicate the required standards and ensure the employee has fully understood them.

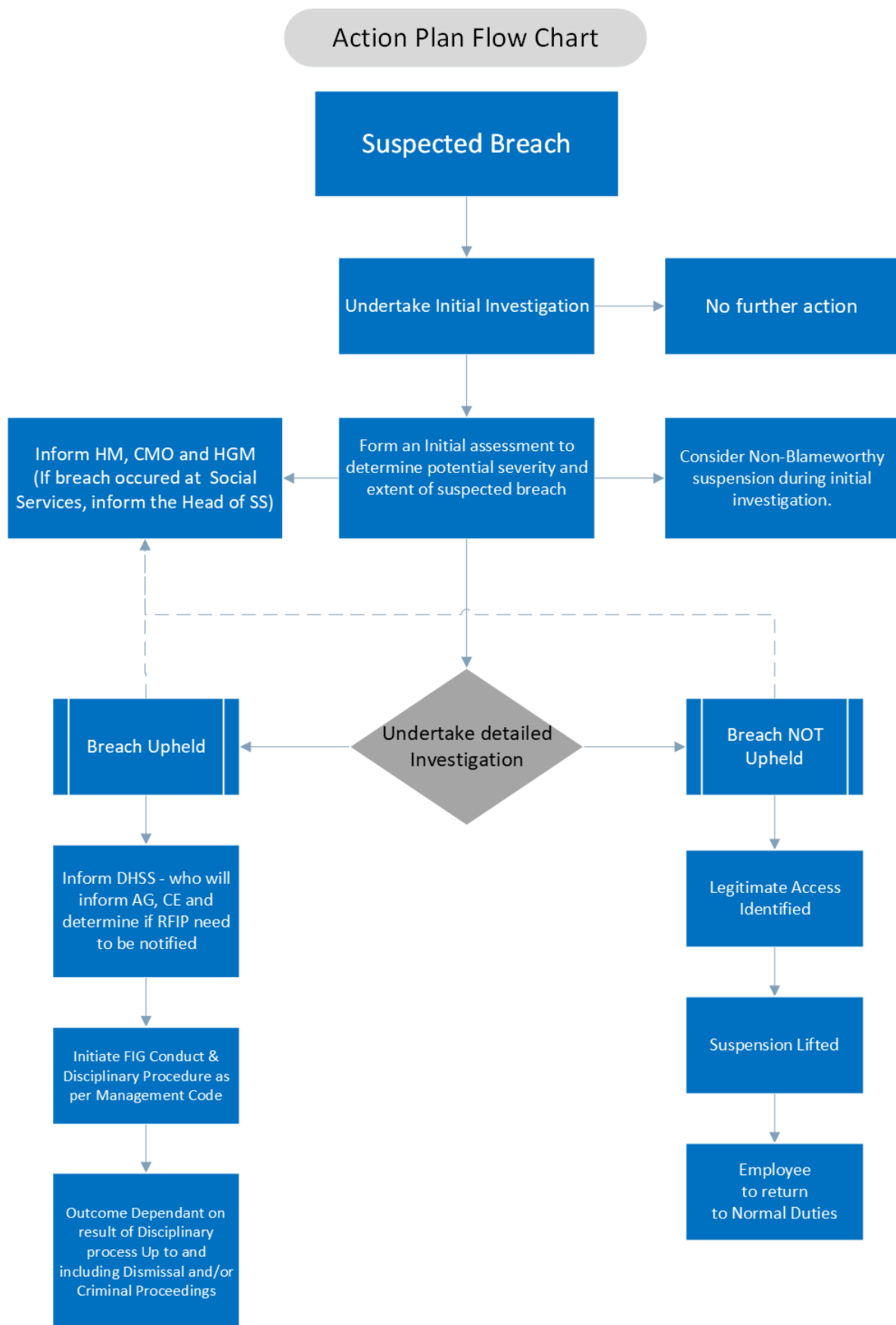
Breach upheld

Line Manager/HoS to inform DHSS, who will ensure the Attorney General and Chief Executive are duly informed as well as potentially RFIP, dependant on the extent and severity of Breach

Line Manager/HoS, if not already in place - consider immediate suspension of employee whilst evidence gathering continues. This may be in the form of a more extensive audit of the EPR system and interviewing other staff.

In circumstances in which a breach is upheld then a 'duty of candour' is owed to the service user to inform them of what has happened. This will ordinarily be communicated to the service user in writing.

The FIG Conduct and Disciplinary Procedure (Chapter 4 of Management Code) will commence.





**Falkland Islands Government
Health and Social Services Directorate**

Code of Confidentiality

All staff, contractors and volunteers working within the Department of Health and Social Services are obliged to comply with the Code of Confidentiality.

Matters relating to patients and their family, their diagnosis, treatment and care, and any other personal information provided to us must be treated in strictest confidence.

All such information must remain within the team to which it was given unless there is justification under the code for sharing it more widely. Where staff members are uncertain about what information can be disclosed and in what circumstances, they should discuss the matter with their line manager or the Chief Medical Officer, Chief Nursing Officer or Director of Health and Social Services. The Caldicott Guardian in the Health Service is the Chief Medical Officer.

Where members of staff 'self-report' incidents during which they have compromised the principles of the Code, a 'no blame' approach will normally be adopted. In these circumstances, disciplinary action will not normally follow. However, where there is a repeated accidental, inappropriate disclosure of any confidential information, either within or outside the Department, this will be treated as misconduct and the Department will take appropriate action under the Management Code. Deliberate breaches, such as gossip, will be treated as gross misconduct, which may result in dismissal.

Any member of staff who is aware of any inappropriate disclosure or breach of the code has an obligation to report it to their line manager or a member of the Senior Management Team. The Whistle-blowing Policy can also be used to raise concerns about confidentiality.

By signing this statement, you are indicating that you have read and understood fully the Code of Confidentiality and confirm that you agree to comply with its contents.

Name and Designation of Staff Member:

Signature:

Name and Designation of Manager:

Signature of Manager:

Date: