NHS Borders

Information Governance

Code of Conduct

Title	**NHS Borders Information Governance Code of Conduct**
Document Type	**Code of Conduct**
Issue no	**2.4**
Issue date	**August 2021**
Review date	**August 2023**
Distribution	
Prepared by	**Ian Merritt**
Developed by	**Ian Merritt**
Equality & Diversity Impact Assessed	

Document Control and Administration

Document revision information

Release	Date	Author	Description of Changes
Version 1	December 2010	Ian Merritt	Released
Version 1.1	March 2013	Ian Merritt	Minor terminology updates
Version 2	July 2014	Ian Merritt	Updated procedures for working outwith NHS premises
Version 2.1	April 2015	Ian Merritt	Added section on Security of Equipment
Version 2.2	September 2017	Ian Merritt	Clarifications and updated references (Data Protection Bill 2017)
Version 2.3	April 2019	Ian Merritt	New section (S5) on GDPR requirements
Version 2.4	August 2021	Ian Merritt	Section on Microsoft 365 added. Other minor clarifications

AUTHORISING CONTROL

Document Control

Document Name:	NHS Borders Information Governance Code of Conduct
Version No:	2.4
Date Created:	August 2010
Date last amended:	August 2021
Authorised by:	Chair of Information Governance Committee
Name:	Lynn McCallum Date: September 2021

Contents

1. Who does this Code apply to?

This Code of Conduct applies to anyone supporting the treatment and care of patients within NHS Borders, that is:

- All staff who are directly employed by NHS Borders.
- Non-directly employed and contracted staff, such as agency staff, volunteers, locums, students on work experience placements and service suppliers.

Independent contractors are expected to apply a similar code of practice in respect of information governance.

All staff providing any services within or on behalf of NHS Borders are also expected to comply with this code and any identified breach will be investigated.

This document should be read and understood before signing the contract of employment or confidentiality agreement statement. If there is anything in this code that is not clear please speak to your manager.

2. What is the Code for?

This Code of Conduct (Code) has been produced to make sure that all staff members are aware of:

a. Their responsibilities and their legal duty to protect the confidential information that they may have access to in the course of their work
b. The correct procedures for handling personal information so that they do not inadvertently breach any of these requirements.

This Code has been written to meet the requirements of:

- The UK General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- Common Law Duty of Confidentiality
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988
- The Public Records (Scotland) Act 2011

3. The NHS Duty of Confidentiality

As an NHS employee or volunteer, you are bound by a legal duty of confidentiality to protect any personal or sensitive information that you have access to or are made aware of during the course of your work. This is a requirement of your contract of employment or confidentiality agreement and also a requirement of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Many health care professionals will also have a duty of confidentiality stated in their profession's own code of conduct.

The duty of confidentiality means you are required to keep any information which may lead to the identification of an individual or could be linked to a specific individual strictly confidential. It applies to information about patients and also information about staff and remains in place even after the individual has died.

4. Definition of Confidential Information

Confidential information can be anything that relates to patients, staff, volunteers, bank and agency staff, locums, student placements, their family or friends.

This information can take many forms including medical notes, audits, employee records, occupational health records, etc.

Confidential information can also be corporate information that is sensitive and not intended to be made public.

Person-identifiable information is anything that may make it easy to identify a person, e.g. name, address, postcode, date of birth, CHI number, National Insurance number etc.

Information may be held on paper or computer files, printouts, videos, photographs, sound recordings or heard by word of mouth.

It includes information stored on portable devices such as laptops, palmtops, CDs and DVDs, USB memory sticks, mobile phones, Dictaphones and digital cameras. People can be recognised from a video or photograph even if their face is not visible.

Certain categories of information are considered particularly sensitive; these include information relating to fertility treatments, sexually transmitted diseases, HIV and termination of pregnancy.

You should consider any information that you use at work, even something as simple as a patient's name and address, to be sensitive and take care to protect it.

Even the fact that a person is attending a hospital or clinic and receiving health care is itself confidential information. Mentioning that you saw someone at hospital could be a breach of their confidentiality.

Appendix 1 details the Information Classification system used by NHS Scotland and the Scottish Government Health Department.

5. Processing Personal Information in accordance with data protection legislation

5.1. General Processing

In order to do anything with personal information (ranging from viewing to storing to deleting and anything in between) the legislation contained within the GDPR and the DPA must be fully complied with.

The GDPR states that all of the following principles must be complied with when processing personal information:

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific, relevant and legitimate purposes;
3. Adequate, relevant and limited to what is necessary;
4. Accurate and where necessary kept up to date;
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed;
6. Processed in a manner that ensures appropriate security of the personal data;

In order to comply with the "lawful" aspect of the first principle, there must be a lawful basis that applies. There are five that are typically available to the NHS:

a. Consent – There is clear consent to process the data
b. Contract – Processing is necessary to fulfil a contract with the individual
c. Legal Obligation – Processing is necessary in order to comply with the law
d. Vital Interests – Processing is necessary to protect someone's life
e. Public task – Processing is necessary to carry out official functions of a public authority

If it is not possible to apply one of the above lawful bases then the processing of personal information must not take place as it would be unlawful.

5.2. Special Category data

Special Category Data refers to information that is more sensitive than other identifiable data and so needs more protection. This is information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

If special category data is to be processed it is necessary to identify both a lawful basis (as above) for general processing and an additional condition for processing this type of data.

There are ten available conditions but the ones most relevant to the NHS are:

- Consent
- Employment purposes
- Vital Interests
- Legal defence
- Provision of Health Care
- Public Health
- Research/Statistical

Bear in mind that if a photograph identifies an individual then it is also likely to identify their race and ethnic origin, which makes this Special Category data.

If you have any concerns about whether personal information should be processed please discuss with the Information Governance team.

6. Accessing information

Each member of staff should only have access to the information they need to do their job. You should not ask for, or expect to be given, information that you are not required to know. If you believe you have excessive access to information than is required for you to perform your job then you should advise your line manager.

It is an offence under the Data Protection Act to obtain or disclose personal information without the consent of the Data Controller.

NHS Borders is the Data Controller. NHS Borders states that personal information for which it is responsible must only be processed for official NHS Borders purposes. Any processing (including viewing) that is not carried out for official NHS Borders purposes is not authorised by NHS Borders and therefore a breach of the Data Protection Act. We take any such breaches seriously.

It is not considered appropriate for a clinician to treat members of their own family. Sometimes it is unavoidable but, in the main, it shouldn't happen. Therefore, there are very few occasions when it is acceptable to view the medical record of a family member. If you ever need to do this legitimately, advise your line manager at the earliest opportunity and before the matter is raised with them by the Information Governance team.

Similarly, it would be highly unusual for a clinician to treat themselves. Viewing your own medical record, without following the Subject Access Request process, is therefore not permitted. All instances of self look ups are reported to management. Your role as a patient is distinct and separate from your role as a clinician. The fact that you are a member of staff does not give you additional rights of access to the data.

If you have concerns about this please discuss with your line manager.

7. Requests for Information about Patients

Requests for information about patients or staff may come from a variety of sources, including staff within the organisation. You should follow these rules:

- Never give out information on a patient to anyone not involved in their care and treatment.
- Don't be afraid to check the identity of the individual requesting the information. If you are not sure who they are or why they want the information, speak to your manager or another more senior person before you disclose anything.
- Where NHS Borders has agreements to share information in order to provide joint care with the local authority, the patient must be informed whenever their information is shared, including who it is shared with.
- If the patient is unconscious and unable to give consent, consult with the health professional in charge of the patient's care before supplying any information.
- NHS Borders has a Subject Access Request Policy in place to handle formal requests from a patient, their advocate or legal advisor for information from their own records. These requests should be forwarded to the Team Supervisor – Subject Access team, Medical Records Department, BGH.
- If you want to use person identifiable information for a reason other than the patient's care, such as research or to contact a patient group for some reason, you must have approval from the Caldicott Guardian. Details can be found on the Information Governance intranet page.

If you have any concerns about disclosing or sharing patient information you must discuss this with your manager or someone with similar standing if they are not available.

7.1. Telephone Enquiries

If a request for information is made by telephone

- always try to check the identity of the caller, and
- check whether they are entitled to the information they request
- take a number, verify it independently and call back if necessary

Remember that even the fact that a person is in hospital, a patient of the hospital/practice, or a member of staff, is confidential. If in doubt consult your manager.

If you take a telephone call asking for information and you think it is suspicious you must report it to your manager at the time, and also record it in Datix, the Incident Reporting System.

7.2. Requests for Information from the Police

Requests for information from the Police should always be referred to the senior manager on duty. There is a specific protocol which sets out when and how information can be shared with the Police. Further information can be found on the Information Governance microsite.

7.3. Requests for Information from the Media

Information should not be given to the press/media under any circumstances. This includes confirming whether an individual is in hospital or works for NHS Borders, however much information the journalist appears to know already.

Only senior managers and/or the Communications Team are authorised to provide information directly to the media.

If you are approached by the media in person or by phone refer them to the Communications Team. See also the NHS Borders Media Relations Policy which is available on the Communications microsite.

8. Carelessness

The most common breaches of confidentiality are caused by carelessness. Some simple rules are:

- Do not talk about patients in public places or where you may be overheard, including corridors and staff canteens.
- Do not leave any medical records or confidential information lying around unattended.
- Make sure that any computer screens, or other displays of person identifiable information, cannot be seen by the general public.
- Make sure you lock your screen when leaving your computer unattended.
- If using shared computers, always log out of clinical systems when leaving the computer.
- Always check meeting rooms for left documents before leaving.
- Close and lock office doors and windows, especially when the building will be unoccupied.
- Don’t disclose door keypad codes to anyone who does not work at that location.

9. Securely transferring information

9.1. Emailing Information

It is not always safe to email confidential information. Most email systems use the internet and are not secure; your e-mails could be intercepted. Identity thieves and other fraudsters look out for emails from specific addresses which may contain information which is useful to them, such as names and addresses etc.

There are secure email systems which you can use and the following table shows which ones you can use for different types of information.

For further information including using email to communicate with patients, please refer to Information Governance microsite or contact the Information Governance team.

9.2. E-mail Guidance Table

nhs.uk – NHS Borders email **nhs.scot** – NHS Scotland email **nhs.net** – rUK NHS email	Public domain / not work related	Work related – Not sensitive **Amber - Protected**		Work related – Sensitive and/or Confidential **Red - Restricted**	
To / From	.uk .net or .scot	nhs.uk	nhs.net nhs.scot	nhs.uk	nhs.net nhs.scot
Another official NHS email address (nhs.net, nhs.scot or nhs.uk)	✓ Subject to policy	✓	✓	✓	✓
Trusted partner meeting government security standards[1] e.g. pnn.police.uk; scotborders.gov.uk; gov.scot;	✓ Subject to policy	✓ Must encrypt	✓	✓ Must encrypt	✓
Trusted partner not meeting government security standards e.g. edu.ac.uk redcross.org.uk nmc-uk.org	✓ Subject to policy	✓ Must encrypt	✓ Must encrypt	✗	✗
Patients and wider public e.g. hotmail.com doctors.org gmail.com	✓ Subject to policy	✓ Subject to policy	✓ Subject to policy	✗	✗
Unconnected organisations	✓ Subject to policy	✗	✗	✗	✗

[1] https://www.gov.uk/guidance/securing-government-email

See **Appendix 1** for a definition of the Information Classification system used in the table above. If the information that you need to send is categorised as "Red – Restricted", consider whether it is appropriate to use e-mail at all.

For guidance on how to encrypt see the Information Security section on the Information Governance microsite (http://intranet/microsites/index.asp?siteid=41&uid=37).

For additional information on sending information between different account types see NHS Borders **Email Security Guidance** and NHS Borders **E-mail Policy** on the Information Governance microsite (http://intranet/microsites/index.asp?siteid=41&uid=2).

9.3. Transporting

Case notes and paper copies of documents should only be sent in envopaks. Other bulky documents should only be transported in approved boxes/envopaks. Dustbin sacks, carrier bags or other containers must not be used.

At no time should boxes of documents or envopaks be left in an insecure area while waiting for collection. Ask the courier to collect them from your office/department or take them to the post room if there is one. The approved boxes/envopaks should only be transported by the approved carrier.

Any **electronic data** being transported should be on an approved, hardware encrypted memory stick. Other electronic media, such as floppy discs/CD/DVDs, should not be used to transport personal information between offices.

9.4. Posting information

If you are sending information by internal or external post to another person or writing about an individual patient or staff member, it should always be addressed to a named recipient, for example the name of the person or a specific post holder, not to a department, unit, or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked 'Addressee Only' or confidential as appropriate. Transit Envelopes should not be used as it is all too easy for the contents to either fall out, or be left in the envelope.

Information sent out using the **external mail** must also observe the rules about packaging and security markings.

Make sure the packaging is strong enough not to tear during transport. Packages should be double wrapped in two envelopes or sheets of packing paper, with the 'confidentiality' marking on the inner packaging only. It is also recommended that you use tamper-evident packaging.

Packages should be sent by Special Delivery or by NHS courier, to make sure that the contents are only seen by the authorised recipient. In some circumstances it is also advisable to obtain a receipt as proof of delivery, such as when sending patient records sent to a solicitor.

Electronic media such as on CD/DVD should be encrypted before posting. Advice on how to encrypt files is available via the IT Service Desk.

9.5. Microsoft 365

NHS Scotland is moving over to the Microsoft 365 platform. This means information that has traditionally been stored on local servers at Health Board premises will instead be hosted in a secure online cloud environment. There are many benefits with this national approach, not least the availability of information from remote, off-site, locations. However, despite the increased accessibility of the information, the same data protection legislation, embodied in the Code of Conduct, applies.

9.5.1. Teams

NHS Borders has rolled out access to Microsoft Teams to all staff. Accounts have been created based on your NHS Borders email address and current network password. Although Teams can be used on personal devices, this option should be a last resort if you do not have access to NHS Borders equipment. Do not share your personal device with anybody else if you have installed Teams on it.

The following points must be complied with:

- Your mobile device must be encrypted and have a strong passcode before you install Teams. Do not allow others to use your mobile device if you have installed Teams on it.
- Make sure you have the latest security patches and anti-malware signatures on your device before accessing NHS Borders files.
- Do not share your network logon password with anybody.
- Don’t save NHS Borders documentation or information to personal devices – that includes mobile devices and desktop or laptop computers.
- While at home you have a personal responsibility to make sure the records and any IT equipment containing NHS Borders data are kept secure and confidential. This means that other members of your family, your friends and colleagues must not use this equipment or be able to see the contents or information on the outer cover of hard copies.
- Be aware of your surroundings when using Teams or other O365 products away from the office. Don’t allow your screen to be overseen by anybody around you.
- If you invite non-NHS staff to a Teams team, they may gain access to more than you are aware of. Carefully review what information will be made available before issuing invitations. If necessary, create a new team for this purpose.
- Any decisions made through discussions in Teams must be recorded elsewhere. This is particularly critical if these are clinical decisions – they must be recorded in the patient record.
- Read the NHS Scotland Acceptable Use Policy for more details - https://www.scot.nhs.uk/AUP

9.6. Faxing Information

Confidential information should never be faxed unless it is to a 'Safe Haven' fax. These are fax machines which are kept in secure and private areas where only a limited number of people can access them. Most clinical areas will have one.

- Remove all staff/patient identifiable data from any faxes unless you are faxing to a Safe Haven.
- Faxes should always be addressed to named recipients.
- Telephone the recipient to inform them that you are sending the fax and ask them to confirm receipt.
- Always check the number to avoid misdialling.
- If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

10. Removing patient records from NHS locations

NHS Borders default position is that patient notes should not be removed from the secure NHS location where they are lodged.

However, it is recognised there are genuine work related reasons why this is not always possible or practical, so specific role-based exceptions may be permitted. Recognised exceptions are detailed below but these must be initially authorised (see note 2) by an appropriate Service Manager, who must ensure there is a compelling and legitimate work reason for this. At all times, the guidance listed in Section 10.3 below should be observed. See the NHS Borders SOP on Transporting Medical Files and Notes for additional guidance if necessary (http://intranet/resource.asp?uid=36329).

10.1. Recognised exceptions

Patient records may be removed from the NHS location where:

- A job function requires the post holder to visit patients in their homes (see note 3)
- A remote clinic is performed at a community based location (see note 4)

When a permitted exception as listed above is authorised, permission only extends to the removal of the patient records for the purposes of the single journey to and from the location where the patient will be seen. Where a series of patient visits will be made on the same day this will count as a single journey, but the guidance in Section 10.3 below must be observed. For clarity, the location a patient will be seen can be

- The patient's home address
- The location of the clinic or
- Any other location as is necessary for the care of that patient.

Note [2] Where the requirement is ongoing (as described above), authorisation is only required the first time. If the circumstances change, re-authorisation must be obtained

Note [3] The post holder can be permitted to convey patient records in these circumstances, using private transport.

Note [4] Where the clinics are scheduled in advance at known NHS locations, the patient records should ideally be transported using the secure courier service and timed to arrive the morning of the clinic.

10.2. Securing the records overnight

The default expectation is that patient records should be returned to the base location at the end of the working day. Where it is not practical or possible to return patient records to the base location, for reasons of distance and/or time, the records should be stored securely overnight at the nearest NHS Borders location. Prior agreement should be obtained from staff at that location so that secure space can be identified and access assured. From this temporary location the records can either be sent via secure courier back to the base location or collected the next day by the staff member for immediate return to the base location. The whereabouts of the patient records must be known by the service at all times.

In exceptional circumstances, and on a case by case assessment, authorisation may be given for patient records to be taken to a staff member's home address: for example at the end of a working day when no NHS secure storage option is available within reasonable distance, or in anticipation of a clinical appointment in a remote location at the very start of the next working day. Authorisation for this lies with the Caldicott Guardian or an Associate Medical Director. If authorisation is received, the staff member is responsible for the security of the case notes while they are in their custody. To that end, the records must remain locked in the provided pilot case, which should ideally be placed in a locked cupboard, if available. Where a lockable cupboard does not exist the case must be placed in such a location that it is out of sight. Nobody, other than the staff member, is permitted to open the case or view the contents.

10.3. Transporting patient records to and from patients' homes as part of ongoing treatment

- Never carry any more records in a vehicle than will be required for the day's appointments/clinics.
- These should be kept in the locked pilot case hidden from view in the boot of the vehicle at all times, other than the single set of records required for the next appointment, which should be kept in the vehicle cabin area (but out of sight) in order to avoid drawing attention to the storage of records in the car boot.
- When records are to be taken into a patient's home they should be removed from the pilot case in the boot prior to the patient's address. After the visit the records should be returned to the secure case in the boot and any new records retrieved if a further patient is to be visited. This procedure avoids drawing attention to the records stored in the boot when the car is about to be left unattended.
- If a planned stop will be made en route to the patient's address, e.g. for fuel, etc., then the records must remain secured in the boot, as described, until ready to depart this location.
- At the end of the session work period take the records to the nearest NHS Borders location and secure them in an office there.
- Records must not remain in vehicles for any longer than is necessary for this purpose. Staff members should avail themselves of secure storage at other NHS Borders locations wherever possible.
- All movements of patient records must be tracked using the standard PAS so that their location and custodian is recorded at all times.

11. Storage of Confidential Information

Paper-based confidential information should always be kept secure, and should be locked away when unattended. Confidential information should not be left in any building or office that is going to be unoccupied for an extended period of time.

Long term archived storage should be considered for records which we are required to keep under the Records Management Policy even when they are no longer being accessed regularly. Specific arrangements are required and should be agreed with the Information Governance team.

Electronic person identifiable information should only be saved onto the NHS Borders networks as these are secure and regularly backed up to prevent data being lost. Information should not be saved to your desktop or laptop computer hard drive. If you are not sure how to save to the server, contact the IM&T Service Desk.

Electronic media e.g. floppy discs, CD and DVDs used within a department should be kept in locked storage. You should keep a record of the contents of each disc and the disposal date.

Any files containing personal information that are stored on external media (e.g. floppy discs, CD and DVDs) should be password protected, and a record of the password should be kept in a separate, secure place as the data could be lost if you cannot remember the password.

12. Disposal of Information

a) Paper-based person-identifiable information, including computer printouts, should be disposed of using the confidential bins provided. Ensure that any unshredded waste is kept in a secure place until it can be collected and taken for secure disposal, i.e. not left unattended in corridors or reception areas.

b) Floppy discs/CD/DVDs containing confidential information must be destroyed by either shredding in an appropriate shredder, or significantly damaging the surfaces of the disc.

c) Computer files with confidential information which are no longer needed should be deleted from both the server and the PC, if necessary.

d) Computer hard disks and USB memory sticks should be sent to NHS Borders IT Services to be destroyed and disposed of. This will generally involve physical destruction to make sure all information is deleted from the disk, as even after deleting and re-formatting it is sometimes possible to bring up the original data again.

13. Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as confidential and must not be given to anyone else.

Passwords should not be written down, so choose something you can remember, but don't use anything that could easily be guessed at, such as your child's name or the system the password relates to. You will be given more information about password control and how to format them when you receive your training and/or password for each system.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. If a previous user has not logged out of a workstation or system then you must log them off and log in with your own credentials before using the system.

Any attempts to breach security should be reported immediately to the Information Governance team. Misuse of passwords may result in disciplinary action and may also breach of the Computer Misuse Act 1990 and/or the Data Protection Act 2018, which could lead to legal action being taken against you.

14. Working at Home

You must have formal approval from your manager to work at home and you must understand that you will be personally liable for any breaches of the Data Protection Act 2018. If any information that could identify an individual is to be removed from an NHS location then the instructions in Section 10 must be followed.

- If you are taking hardcopy documents or files home, make sure there is a record of what you have taken, where you are taking them and when they will be returned.
- It is not permitted to connect to a personally owned printer or print any NHS Borders documentation at a remote working location.
- Patient case notes should only be taken home in exceptional circumstances, and explicit agreement given by the Caldicott Guardian, or an Associate Medical Director. Where this has been approved, Medical Records must also be informed in case the notes are required for patient care or to respond to a Subject Access Request. See section 10 for full details.
- Any personal information on paper documents must be placed in a sealed container, e.g. an envopak, before being taken out of NHS Borders buildings.
- Make sure any paper documents or electronic devices are locked in the boot of the car or carried on your person while being transported from your work place to your home. They must be secured in the boot of your car before your journey commences. See section 10 for full details.
- Under no circumstances should any NHS Borders documents/case notes/diaries, personal data, or IT equipment be left on view in an unattended vehicle. Items should be transported in the boot of the vehicle and if the vehicle is being left, then the items should be removed for safekeeping. See section 10 for full details.
- If working on a computer at home, you must use an NHS Borders encrypted laptop. Under no circumstances should you use your own computer. **Be aware that any corporate information stored on your home computer (including your personal e-mail address) is still subject to release under the Freedom of Information Act**.
- When using USB memory sticks, only NHS Borders approved, encrypted devices must be used. These can be ordered through the IM&T Service Desk. It is your responsibility to make sure you keep your USB memory stick safe and report it if you lose it. Remember, USB Sticks are to be considered corporate items, not personal issue, and must be redeployed before a new purchase is considered.
- If you take computer records home on a USB memory stick you must NOT put this information onto your personally owned computer.
- While at home you have a personal responsibility to make sure the records and any IT equipment are kept secure and confidential. This means that other members of your family, your friends and colleagues must not use your computer equipment or be able to see the contents or information on the outer cover of the records.
- Do not dispose of any confidential waste at home. It should be brought back to your workplace and disposed of properly there.

15. Security of Equipment

Staff members are responsible for the safekeeping of any items of equipment issued to them, or used by them, to carry out NHS Borders business. In the context of this Code of Conduct, this relates to any piece of equipment used to store or process information including (but not restricted to) desktop, laptop or tablet computers; mobile phones; Dictaphones (digital or tape); USB memory sticks or any other storage medium; etc.

In the event that a piece of equipment is lost or stolen and there is, *or there has been*, NHS Borders information stored on it then an incident must be recorded in Datix. In addition, the event must be logged with the IM&T Service Desk for the attention of the Information Governance team. Full details of the information stored on the device must be passed to the Information Governance team, including the level of sensitivity/confidentiality of the information based on the scale described in Appendix 1 and whether the device was encrypted or protected by a passcode. If a physical or information asset has been stolen, this must be reported to the police.

16. Copying Software

It is important that software on the PCs/systems used for work purposes is not copied and used for personal use. All computer software used with NHS Borders is regulated by licence agreements and must not be copied onto any personal computers. Copying the software is illegal and could lead to legal action against NHS Borders and/or the person who copied the software.

17. Social Media

Social media has become an everyday form of communication, both in the workplace and for personal use. This Code applies to NHS Borders employees using social media for personal use. No information which may lead to the identification of individual staff or patients or information about NHS Borders business should be posted through social media sites.

Use of NHS Borders social media sites is managed by the Communications Team who will provide access for staff to use as appropriate.

18. Contacts

If you have any queries about the information in this Code of Conduct, and how it applies to you, you should discuss it with your line manager in the first instance or with the NHS Borders Information Governance team or the Caldicott Guardian (contact details are provided on the Information Governance microsite).

19. Non-compliance

Non-compliance with this Code of Conduct by any person working for NHS Borders may result in disciplinary action being taken in accordance with NHS Borders Management of Employee Conduct Policy, and may lead to dismissal for gross misconduct.

20. Amendments

This code will be amended as necessary to reflect the NHS Borders development of policies and procedures and the changing needs of the NHS.

Appendix 1: Information Classification

GREEN: Unclassified information

This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation if lost of disclosed to unintended recipients. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person's physical or mental state.

AMBER: Protected information

In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

- Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost.
- Any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result).
- Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).

RED: Highly sensitive information

Most boards also hold some information which is highly sensitive. Particularly:

- Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way).
- Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health.
- Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file).
- Information relating to vulnerable persons' health (e.g. child protection cases)
- Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment).
- Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Appendix 2: Confidentiality Statement

For the following to sign:

- Employees of NHS Borders
- non-directly contracted personnel such as agency, locums, student placements, service suppliers

The Confidentiality Statement can be found on the NHS Borders Intranet on both the Information Governance site under Policies & Procedures (http://intranet/microsites/index.asp?siteid=41&uid=2) and the Human Resources site. http://intranet/microsites/index.asp?siteid=57&uid=89

A sample of the statement is provided on the following two pages.

CONFIDENTIALITY STATEMENT

In the course of your duties you may have access to confidential information about patients, members of staff or other health service business. Failure to observe the following rules will be regarded as serious misconduct which will result in disciplinary action being taken against you, including possible dismissal.

Patient Information

On no account must information relating to patients be accessed by or divulged to anyone other than authorised persons - for example, medical, nursing or other professional staff, as appropriate, who are concerned directly with the care, diagnosis and/or treatment of the patient. If you are in any doubt whatsoever as to the authority of a person or body asking information of this nature you must seek advice from your senior officer. All patient information should be treated in accordance with the NHS Code of Confidentiality Guidelines and the Caldicott Recommendations.

Staff Information

Similarly no information of a personal or confidential nature concerning individual members of staff should be accessed by or divulged to anyone without the proper authority having first been given.

NHS Borders Information

The unauthorised disclosure of official business under consideration by NHS Borders or one of its Committees by an employee of NHS Borders is also regarded as a breach of confidence and may lead to disciplinary action.

Information Technology & Data Protection

You should make yourself familiar with the following list of key policies regarding confidentiality and associated issues which can be found on the intranet (http://intranet)

- NHS Borders Data Protection Policy
- NHS Borders IT Security Policy
- NHS Borders E-Mail Policy
- NHS Borders Internet Policy

You should be particularly aware that any wilful misconduct, such as unauthorised amendments, deletion or copying of data, or negligence, such as introducing a 'computer virus' by loading unlicensed or unauthorised software or unscreened floppy disks to computers, computer systems, or data in your care or control will result in disciplinary action. Such misconduct or negligence may also result in you being personally charged with committing a criminal offence under the following UK Acts:

- The Data Protection Act, 2018
- Copyright Designs and Patents Act, 1988
- Computer Misuse Act, 1990

General Considerations

Under no circumstances should any interviews be given to any members of the press or media or any information passed to them without written approval of a senior executive member of NHS Borders. (See following exception for Medical staff.)

Medical Staff

It is recommended that Medical staff should not give interviews to any members of the press or media nor pass any information to them without written approval of a senior executive member of NHS Borders. This does not in any way negate the rights conferred under Para 12.1.1 of the Terms & Conditions of Service of the 2004 Consultant Contract, but should be seen as protection against aggressive requests from the media.

Voicing Concerns

This statement does not prevent staff from raising concerns provided the NHS Borders Whistleblowing Arrangements policy or NHS Borders Grievance policy is followed. Concerns may also be raised using the National NHS Scotland Confidential Alert Line on 0800 008 6112 which available to all staff.

I hereby certify that I have read and understood the above statement and the NHS Borders Information Governance Code of Conduct regarding the confidentiality of information relating to patients, members of staff and health service affairs. I also authorise use of, and agree to any scanning of, all of my personal e-mail messages as stipulated in the NHS Borders Email policy.

Full Name (Print): .....Signature: .....

Designation: .....

Date: .....

Please return a copy of the signed and dated statement to your supervisor/line manager who will give you a copy and send a copy the HR Department

The Six Data Protection Principles

1. Personal data shall be:

    a) processed **lawfully**, **fairly** and in a **transparent manner** in relation to the data subject ('lawfulness, fairness and transparency');

    b) collected for **specified, explicit and legitimate purposes** and **not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    c) **adequate**, **relevant** and **limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

    d) **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    e) **kept** in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

    f) processed in a manner that ensures **appropriate security** of the personal data, including **protection against unauthorised** or **unlawful processing** and against **accidental loss**, **destruction** or **damage**, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

The Caldicott Recommendations

Principle 1	Justify the purpose(s) of accessing and/or using information
Principle 2	Don't use patient-identifiable information unless absolutely necessary
Principle 3	Use the minimum necessary patient-identifiable information
Principle 4	Access to patient-identifiable information should be on a strict 'need to know' basis
Principle 5	Everyone should be aware of their responsibilities
Principle 6	Understand and comply with the law
Principle 7	The duty to share information can be as important as the duty to protect patient confidentiality

Appendix 3: Confidentiality Statement – Volunteers

For volunteers to sign

The Confidentiality Statement for volunteers can be found on the NHS Borders Intranet on both the Information Governance site under Policies & Procedures

http://intranet/microsites/index.asp?siteid=41&uid=2

and the Volunteering site.

http://intranet/microsites/index.asp?siteid=430&uid=7

A sample of the statement is provided on the following page.

CONFIDENTIALITY STATEMENT – VOLUNTEERS

As a volunteer in NHS Borders you are bound by a code of confidentiality. Simply stated this means that *anything you see or hear while volunteering must not be discussed or talked about with anyone outside* i.e. your partner, spouse, friends, relatives etc.

It is a privilege to be given access to others people's private concerns, from information about their health and welfare, to information about personal possessions and family members.

Patients may on occasion offer 'in strict confidence' important information about themselves or a difficult situation at home or with friends. This may be of a potentially serious nature and volunteers should never be put in the position of keeping "secrets".

If you find yourself faced with this you should make it clear to the patient that you have to share the information with a member of staff. These individuals carry overall responsibility for the wellbeing and safety of patients. This should be clearly explained to show an understanding of any perceived breach of trust and to explain why it is necessary to disclose personal information.

To enable the best service to be provided, there is a need for sharing of personal information amongst staff and volunteers. Limits to this will have been decided by the clinical staff on the ward or unit.

NHS Borders has a legal duty to ensure compliance with the policy on confidentiality of personal information.

Confidentiality is fundamental to all work in the NHS and is so important that any volunteer breaking the code will no longer be considered appropriate for volunteering.

I have read and understood the above and agree to abide by the NHS Borders policy on confidentiality.

Print (full name) : Signature :

Date :

Please return a copy of the signed and dated statement to your supervisor/line manager who will give you a copy and send a copy the HR Department

Appendix 4: Confidentiality Statement – Workplace Tours

Workplace tours within NHS Borders provide young people and children with the opportunity to observe the delivery of health care before entering the world of work

For workplace visitor to sign

The Confidentiality Statement for workplace tours can be found on the NHS Borders Intranet on both the Information Governance site under Policies & Procedures *http://intranet/microsites/index.asp?siteid=41&uid=2* and the Human Resources site. http://intranet/microsites/index.asp?siteid=57&uid=92

A sample of the statement is provided on the following page.

CONFIDENTIALITY STATEMENT – WORKPLACE TOUR

Most people are quite private and sensitive about their health, and in the NHS we take great care to ensure that we treat all patients with respect and privacy. For this reason, confidentiality is very important to us.

In the course of your workplace tour you may have access to confidential material about patients, members of staff or other health service business. You can discuss where you have been and what you have experienced when on workplace tour but you must not discuss any information that could identify, or be directly linked to, a patient with your friends, family or school. If you fail to observe NHS Borders rules on confidentiality, your workplace tour may be terminated and your school will be informed.

Patient information

On no account must information relating to patients be shared with anyone other than authorised persons - for example, doctors, nurses or other professional staff, who are concerned directly with the care, diagnosis and/or treatment of the patient. If you are in any doubt whatsoever about the authority of a person asking for information of this nature then ask your mentor/supervisor.

Staff information

Similarly, no information of a personal or confidential nature concerning individual members of staff should be shared with anyone without permission from your mentor/supervisor.

Board information

The unauthorised disclosure of official NHS Borders business is also regarded as a breach of confidence and may lead to termination of the workplace tour.

Information Technology & Data Protection

You should be particularly aware that any wilful misconduct, such as unauthorised amendments, deletion or copying of data, or negligence, such as introducing a 'computer virus' by loading unlicensed or unauthorised software or unscreened floppy disks to computers will result in termination of the workplace tour. Such misconduct or negligence may also result in you being personally charged with committing a criminal offence under the following UK Acts:-

- The Data Protection Act, 2018
- Copyright Designs and Patents Act, 1988
- Computer Misuse Act, 1990

General considerations

Under no circumstances should any unauthorised interviews be given to any members of the press or media or any information passed to them without written approval of a senior executive member of NHS Borders.

I hereby certify that I have read and understood the above statement regarding the confidentiality of information relating to patients, members of staff and health service affairs.

Full Name (Print) : Signature :

Designation : **Workplace Tour Student** Department :

Date :

Please return a copy of the signed and dated statement to your mentor/supervisor who will give you a copy and send a copy the HR Department