FairWarning Guidance for Users of Clinical and Patient Management Systems

Document Control

	Date
Ratified	
Reviewed	
Next Formal Review	
Document Location	

Authorisation Following this Review

	Date
Ratified by Staff Governance Committee	
Placed/Replaced on the Intranet/Extranet	

This Version History

	Date
Impact assessed	
Executive Team	
Staff Consultation	
Partnership Forum	
Staff Governance Committee	

Contents

1.0 Introduction

NHS Health Boards collect and uses considerable quantities of special categories of personal information for clinical, administrative, research and planning purposes, each of which contributes to the services patients receive.

We must respect the privacy of the individuals that this data relates to, but equally the information is of no value unless it is readily available to staff that need it in order to provide healthcare or other supporting services. When accessing personal information, we must strike the right balance between the need to access information and the need to keep it secure and confidential.

The security of patient information within health services has been given a high profile in recent years and the Information Commissioners Office (ICO) has the ability to fine organisation up to £17.5 million for serious breaches.

To assist health boards in continuing to keep patient information secure and confidential, the Scottish Government has provided all NHS Scotland Health Boards with Privacy Breach Detection Software. This software, FairWarning, can analyse activity on our clinical and patient management systems and report on instances where potentially, unauthorised access has occurred.

2.0 Purpose

The purpose of this guidance is to remind all users of clinical and patient management systems of their responsibility to keep personal data secure and confidential at all times and provide information on what constitutes unauthorised access.

3.0 Scope

This guidance covers all patient information held and processed by NHS Health Boards and GP Practices. It is applicable to all users of clinical and patient management systems.

4.0 Definition of Terms

4.1 Information Commissioners Office (ICO)

The ICO are the supervisory body and regulator with regards to the Data Protection Act 2018, EU General Data Protection Regulation (GDPR) and Freedom of Information in England.

4.2 Personal Data

The ICO define personal data as information relating to a natural person who:

- can be identified or who are identifiable, directly from the information in question; or

- who can be indirectly identified from that information in combination with other information.

4.3 Special Categories of Personal Data

Special category data is personal data which data protection legislation says is more sensitive, and so needs more protection, for example, information about an individual's health, race, religion, sexual orientation or trade union membership.

4.4 Unauthorised Access

Examples of unauthorised access to patient information include:

- **Accessing the records of people of media interest:** unauthorised or unnecessary examination of the records of people in the public eye – for example, footballers or sports stars, politicians, criminals, media personalities or people who have featured in the press.

- **Accessing patient information where you do not have a legitimate reason for doing so:** This might include accessing the records of colleagues, friends, your children, other family members or neighbours. This access may be malicious and / or simple curiosity. It may even be at the request of the individual. All represent unauthorised access and constitute a breach which will be flagged by the FairWarning system.

- **Accessing your own record:** You must make a Subject Access Request under data protection legislation if you want to access your own information. If you need to check or change an appointment you should not access your record to do this.

- **Logging on as someone else:** Using the login of another member of staff, even in the course of treating a legitimate patient, may constitute a breach of the appropriate IT Policy and will be investigated accordingly.

5.0 Roles & Responsibilities

5.1 Users of NHSScotland's Electronic Systems

You must be aware of your responsibilities with regard to confidentiality and accessing personal information.

You must only access information that you need to know in order to carry out your legitimate administrative/clinical duties.

Never leave your computer logged on and unattended.

Never share your passwords.

5.2 Responsibilities of those authorising access

Ensure that users of clinical and patient management systems are only granted access to information which they need to know.

Ensure that access is revoked when it is no longer needed.

Ensure that users of clinical and patient management systems who change departments have their access to systems reviewed.

Ensure that where users of clinical and patient management systems have accessed information inappropriately that this is dealt with effectively.

6.0 Information Assurance

Information governance refers to the practice of handling information in a confidential and secure manner, following appropriate ethical and quality standards. Information governance standards are modelled around HORUS principles:

Holding information securely and confidentially
Obtaining information fairly and efficiently
Recording information accurately and reliably
Using information effectively and ethically
Sharing information appropriately and lawfully

Information governance is fundamental to the effective delivery of health care services particularly as we move towards the introduction of electronic personal health records.

7.0 Confidentiality

NHS Health Boards and GP Practices take confidentiality and data protection responsibilities very seriously. Patients entrust staff with, or allow staff to gather, special category data relating to their health and other matters as part of seeking their treatment. They do so in confidence and have a legitimate expectation that we will respect their privacy and act appropriately.

Confidentiality is about ensuring that only relevant patient or service user information is accessed or shared with those who have a need to know, when it is appropriate to know.

All NHS staff are subject to a common law duty of confidentiality and must abide by this. As a general principle, this duty of confidentiality arises when a person receives information in circumstances where he/she knows or can be taken to know, that the information is to be treated as confidential – this includes demographic [relating to patient name, date of birth, address etc] and administrative data as well as clinical data.

Confidentiality is a legal obligation and is a requirement established within professional codes of conduct. All NHS employment contracts contain a specific clause relating to

confidentiality, staff who breach this principle may be subject to disciplinary procedures and legal proceedings.

8.0 FairWarning

The FairWarning system detects potential instances of unauthorised access to patient information held within electronic information systems and is the means by which we can assure patients, members of the public and the Information Commissioner that the information we hold is handled correctly and in accordance with the law.

The system tracks electronic systems in real time and:

- Flags potential unauthorised access to patient information
- Highlights unusual or suspicious activity
- Enables investigation of accesses to specific patient records
- Enables investigation of accesses made by specific staff members

Every time you access a record it can be traced back to you and you could be asked to provide an account to demonstrate that you had a legitimate reason for accessing the record.

If you are in any doubt as to whether access would constitute a breach of these rights, ask yourself: “Do I need to know this information in order to do my job?” If the answer is no, don’t access it. See Appendix 1 for common scenarios and guidance on the actions that should be taken.

9.0 Consequences of inappropriately accessing information

It has always been part of your Terms and Conditions of Employment that access to patient information is on a strictly need-to-know basis. FairWarning simply allows us to flag potential breaches more easily.

Inappropriate access to patient information is an abuse of your privileged position as a user of the clinical and patient management systems, even if the patient information is accessed with good intentions. Users accessing patient information without a legitimate administrative or clinical reason face serious consequences and may be subject to their employer’s Management of Employee Conduct Policy/Disciplinary Policy.

NHS staff members accessing patient information without a legitimate administrative or clinical reason may be referred to Human Resources for consideration of any mitigation and to form a view as to whether the matter can be appropriately dealt with through an informal supportive improvement plan or progressed to a formal investigation.

Other users of the health board’s clinical and patient management systems who access patient information without a legitimate administrative or clinical reason will be referred to their employer/further education establishment for consideration of any mitigation and to decide on the best course of action.

Users of clinical and patient management systems should also be aware that the ICO have the power to prosecute individuals that inappropriately access patient records.

10.0 Related Documents

10.1 Local

- NES Corporate Information Security Policy
- NES Data Protection, Confidentiality and Privacy Procedures
- NES Data Breach Notification Management Procedure
- NES We want to give you FairWarning (link to be provided)
- NES FairWarning Manager's Guide (link to be provided)
- NES NES FairWarning Staff Guide (link to be provided)
- NES Management of Employee Conduct Policy: Disciplinary Policy and Procedures

10.2 National

- Caldicott Principles
- Data Protection Act 2018
- EU General Data Protection Regulation
- Protecting Patient Confidentiality: NHSScotland Code of Practice
- Accessing Personal Information on Patients and Staff: A Framework for NHSScotland

11.0 Appendices

Appendix 1 – Scenarios and Actions

Appendix 1 – Scenarios and Actions

The scenarios below provide further guidance.

Scenario	What should I do	Who should I notify
I've just seen a patient who was on the front page of the local paper this week; I wonder what they're doing here?	Idle snooping at patient information is a serious breach of confidentiality. You should only access records when you have a legitimate reason to do so.	
My family member has asked me to check their appointment date.	Advise your family member to contact the department responsible for making the appointment to check their appointment details. You should not access the record yourself.	
I attend hospital services and have not received/have lost/forgotten my appointment letter.	You should contact the department responsible for making the appointment; they will be able to advise if a referral has been received and if an appointment has been arranged. They can also confirm the appointment details (including date, time, location and care giver) and send another appointment letter if required. You should not access your own record to check this information	
I am on duty and a friend or relative arrives in the department or ward that I am working in.	Wherever possible you should ask a work colleague to attend to the patient. If this is not possible you should go ahead and deal with the patient in the normal way.	You should e-mail your line manager advising them of the date and time when you dealt with the patient.

Scenario	What should I do	Who should I notify
I am required to treat or process information about a friend or relative as part of my role.	Wherever possible you should ask a work colleague to treat the patient or process the information. If this is not possible you should go ahead and deal with the patient/information in the normal way	You should e-mail your line manager advising them of the date and time that you saw the patient and/or processed the information.
I attend hospital services and my address and telephone number have changed.	The receptionist at the clinic you attend will be able to tell you what demographic information is recorded about you (including name, address, contact telephone numbers, D.O.B, CHI number and GP). They will also be able to update any information that has changed. You should not access the record yourself to check or amend details.	
My friend or relative is attending hospital services and has asked me to check their test results.	You should advise your friend or relative to contact their GP or the Medical Secretary of the Consultant who is responsible for their care who will be able to advise if their results are available and answer any questions they may have. You should not access the record yourself even if it is just to check if the results are available.	
I need to contact a friend or relative urgently, I wonder if there is an up to date telephone number on their patient record.	You must not access a friend or relative's health record to check contact details; this would be considered a breach of conduct and may result in disciplinary action.	

Scenario	What should I do	Who should I notify
I am attending hospital services; my GP/Consultant is aware that I work in the Hospital environment and has advised me to check my test results myself.	You should not access your own records to check results. Using a log on given for work purposes to access your own records is a breach of conduct and may result in disciplinary action. You should advise your GP/Consultant that you are not allowed to do this and contact them to receive your results in the same way as any other patient would.	
A new colleague is unsure of how to use the computer system and has asked for my advice.	You should not access your own/your relatives records to practice/train colleagues on the computer system. If you or a colleague require further training on the computer systems, you should contact your line manager to seek advice or arrange further training.	
I attend hospital services and have an appointment in the department that I work in. I have been asked to print labels for my upcoming appointment	You should advise that you are not allowed to access your own health record and another member of staff in the department should print the labels. You should not access your own record to print labels.	

The above scenarios are not exhaustive and in cases of doubt you should contact your line manager for advice.