

# Manager’s guide

**Fairwarning**



## Inappropriate access to Health Records

### (including FairWarning Alerts)

The security of patient data within health authorities has been given a high profile

in recent years. The Information Commissioner’s Office has increased powers, including the power to fine organisations up to £17.5 million or 4% of their annual turnover for serious breaches. The negative effect on our organisation’s reputation could have an even greater impact than a monetary fine.

To assist NHS Boards in continuing to keep patient information secure and confidential, the Scottish Government has provided all NHSScotland Boards with Privacy Breach Detection software.

This software, FairWarning®, can be linked to all of our clinical and staff systems, can analyse activity on our clinical systems, and can report on instances where potentially inappropriate access has occurred.

Examples of this include users looking up records of colleagues, family members, neighbours or even their own records.

The introduction of FairWarning® does not mean any changes for staff. It has always been a condition of employment that access to clinical records is on a strictly need-to-know basis and the NHSScotland Code of Practice: Protecting Patient Confidentiality reiterates this.

Staff are provided with information on how to use electronic systems and sign a declaration that they have read relevant governance statements before gaining access to our network. FairWarning® is therefore simply the means by which we can assure our patients, the Board and the Information Commissioner that the information we hold is handled correctly and in accordance with the law.

As a manager, you must ensure that all of your staff members are fully aware that patients’ health records must only be viewed if there is a clinical or business requirement to do so. This means staff must **not be accessing records inappropriately; for example: looking at their own health record** (even to confirm that a clinical system is working correctly or to check test results) **or the records of family, work colleagues, friends, acquaintances** and so on, unless it is a requirement of their job to do so. You should also inform new staff members that they must not use details of family, friends or colleagues for practice or training on a new system.

If a member of staff wants to view their own health records, or those of a dependent relative, they must follow the same process as any member of the public, i.e. the Subject Access Request process as stipulated in the Data Protection Act 2018. Guidance on this process can be provided by the Data Protection Advisor or the Health Records Manager.

### FairWarning Alerts

Information Governance will send you a report if FairWarning identifies any potentially suspicious activity that has been performed by a member of your staff. The type of activity that may generate a report includes, but is not restricted to, viewing their own record or that of a member of their family, a neighbour or a work colleague.

If you, or any member of staff, has a specific concern about who may have been accessing a particular health record, then Information Governance can produce

a tailored report for you. This will only be granted if authorised by a line manager/ Director and a clear appropriate reason provided.

When you receive this alert, you must check whether there is a legitimate clinical or business reason for the staff member to have accessed these records. If there is, this is known as a “False Positive” and you must report this back to the Data Protection Advisor, explaining why this is a False Positive, e.g. Medical Secretary typing a letter to a neighbour receiving treatment through the specialty they work in. If you do not give sufficient information, the Data Protection Advisor may contact you for further clarification. The False Positives are then removed from the reports and no further action taken.

The introduction of FairWarning® makes absolutely no change to existing laws or policies regarding access to patients’ health records. These **must only be accessed if there is a clinical or business requirement to do so**. A member of staff’s ability

to access health records does not automatically grant them the right to do so. FairWarning® will simply identify instances where staff privileges may be being abused.

This document is intended to offer general guidance in the event you receive a FairWarning® alert related to one of your staff members. It is essential, for the benefit of all concerned that the guidance is applied consistently in all cases, regardless of the position or designation of the staff member involved. Compliance with the Data Protection Act is a legal requirement and NHS Greater Glasgow & Clyde must be able to demonstrate that non- compliance is dealt with appropriately.

For more detailed advice, you should contact the Data Protection Advisor.

|  |  |  |
| --- | --- | --- |
| **Potential Staff Breach (identified by FairWarning System)** | **Potential (Inappropriate) Reasons for Breach** | **Expected Management Action** |
| Staff Member accesses own health records | * To check if their personal

data is accurate* To update record, i.e. change of address
* To check date/ time of an upcoming appointment
* To access lab results/check diagnosis
 | The manager must determine whether the staff member had a legitimate work reason to access their own record,i.e., filing or transferring files. If there is a legitimate reason, the manager should report back to the Data Protection Advisor that this was a False Positive result and the reason why. No further action should be taken.If there is no obvious work related reason for the staff member to access their own record, the manager should arrange to meet with the member of staff and explain why this is a breach of NHSGGC Policy and inform the staff member that any further breaches may be dealt with in line with the NHSGGC Disciplinary Policy & Procedure: Management of Employee Conduct.Actions* The manager should complete a Record of Discussion form (see Appendix A) and store in the staff member’s personnel file;
* The member of staff will be asked to access the

E-Health section on Staffnet and read the information about FairWarning;* The member of staff will be asked to complete the on-line e-learning module about ‘Safe Information Handling’ (unless this has recently been undertaken).
* The manager must complete a DATIX form to formally record this breach of the Information Governance Standard/ Patient Confidentiality.
 |

|  |  |  |
| --- | --- | --- |
| **Potential Staff Breach (identified by Fair Warning System)** | **Potential (Inappropriate) Reasons for Breach** | **Expected Management Action** |
| Staff Member accesses someone else’s health recordse.g. child or other family member/ neighbour/ colleague/high profile individual, etc. | * To check if personal data is accurate
* To update record

i.e. change of address* To check date/ time of an upcoming appointment (either for self or for a third party)
* To access lab results / check diagnosis
* Checking address/ phone number for personal reasons
* Checking to find out if a pregnant colleague has had their baby.
* Practicing on a system using familiar names.
 | The manager must determine whether the staff member had a legitimate work related reason to access the record(s) in question. If there is a legitimate reason, the manager should report back to the Data Protection Advisor that this was a False Positive result and the reason why. No further action should be taken.If there is no work related reason for the staff member to access the medical records, the manager may contact the Data Protection Advisor and ask for a more detailed report of the staff member’s electronic activity over a specified period, (e.g. three months),to ascertain whether there have been any further breaches.* The manager should complete a DATIX form to formally record this potential confidentiality breach.
* When the detailed report has been obtained and analysed, the manager should contact the Human Resources Support and Advice Unit to arrange an Investigatory Meeting with the member of staff in line with the Disciplinary Policy & Procedures: Managing Employee Conduct.
* If there has been only one breach and the staff member is able to provide a reasonable explanation, it may be appropriate to remind the staff member of their responsibilities without arranging for a formal Investigatory Meeting. The same steps would then be taken as when someone accesses their own records. The manager should also advise them that any further breaches will be managed in line with the Disciplinary Policy & Procedures: Managing Employee Conduct.
* If there is historical evidence that the staff member has inappropriately accessed patient records,

and they are unable to provide a satisfactory explanation, a decision may be taken to refer the case to a disciplinary hearing in line with the Disciplinary Policy. |



|  |  |  |
| --- | --- | --- |
| **Potential Staff Breach (identified by Fair Warning System)** | **Potential (Inappropriate) Reasons for Breach** | **Expected Management Action** |
|  |  | Each case must be fully explored and dealt with appropriately, dependent on the individual circumstances. However, in a case where a staff member has inappropriately accessed patient records on more than one occasion, this should be investigated under the NHSGGC Disciplinary Policy & Procedure: Management of Employee Conduct. Dependent on the facts uncovered, this may result in referral to a disciplinary hearing.Where it can be evidenced that a staff member has repeatedly accessed the health records of others, there is an expectation that this would be dealt in line with the NHSGGC Disciplinary Policy & Procedure: Management of Employee Conduct. In line with the Board’s Data Breach Policy, the outcome of the investigation and any sanction levied against the staff member should be reported back to the Information Governance Department. |

|  |  |  |
| --- | --- | --- |
| **Potential Staff Breach (identified by FairWarning System)** | **Potential (Inappropriate) Reasons for Breach** | **Expected Management Action** |
| Staff Member shares information they can only know as a result of their employment, or accesses someone else’s health recordsand shares the informationwith a third party.For example:A member of staff looking up a colleague’srecord to see why they are off sick and sharing this information with another member of staff. | * At the request of a third party, e.g. family member asking for confirmation that someone is pregnant

or received treatmentin ED.* Checking a colleagues record to find out why they are absent from work.
* Checking the record of a ‘high profile’ individual and sharing information with a third party.
 | In the event that a member of staff is suspected of sharing any information with a third party, a full investigation should be carried out in line with the NHSGGC Disciplinary Policy & Procedure: Management of Employee Conduct.Where it can be evidenced that a staff member has inappropriately accessed the health records of others, there is an expectation that this would be dealt with in line with the NHSGGC Disciplinary Policy & Procedure: Management of Employee Conduct.In particularly serious cases, or where a previous warning has been issued, employment may be terminated following a formal investigatory process and disciplinary hearing. |