Emergency Care Summary System

Information Governance Guidance for Pharmacy Managers

Fairwarning & Inappropriate access to Personal Information

Last Update – March 2020

1. Background

The security of patient data within health boards has been given a high profile in recent years and the Information Commissioner's Office now has increased powers, including the power to fine organisations. The fines can now be up to 20 million euro/17 million pounds for serious breaches. However the negative effect on the organisation's reputation would arguably cause greater damage than a monetary fine.

To assist Health Boards in continuing to keep personal information secure and confidential, the Scottish Government has provided all NHS Scotland Health Boards with Privacy Breach Detection software, called Fairwarning.

The Fairwarning system can be linked to clinical and staff systems and can be used to analyse activity on our systems and report on instances where potentially inappropriate access has occurred.

Looking at any record which the user has no legitimate clinical or administrative reason to be viewing is considered inappropriate. Specific examples include system users looking up records of colleagues, family members, neighbours or even their own records. A member of staff's ability to access personal information does not automatically grant them the right to do so.

Fairwarning automates the auditing and alerting system which may prompt an investigation. Access to personal information is on a strict need-to-know basis. The NHS Code of Practice on Protecting Patient Confidentiality which every member of staff is required to adhere to, reiterates this. Fairwarning is an additional means by which we can assure our patients, staff, the NHS Board and the Information Commissioner that the information we hold is handled correctly and in accordance with the law.

1. Management Action

As a manager of staff, you should ensure that your staff members are fully aware that, in particular, personal information should only be viewed if there is a clinical or administrative reason to do so. This means staff shouldn't be accessing records inappropriately; for example: looking at their own health record (even to confirm that a clinical system is working correctly, to check test results or appointments), the records of family, work colleagues, friends/acquaintances and so on, unless it is a requirement of their job to do so, we always recommend where practical you ask another colleague to administer activities which are for family members, friends/acquaintances. Staff members must not use details of family, friends or colleagues for 'practice' or training on the system.

If a member of staff wishes to view their own health records, or those of a dependent relative, they must follow the same process as any member of the public by following the Subject Access Request process as stipulated in the GDPR and Data Protection Act 2018. Guidance on this process can be obtained from the NHS Ayrshire & Arran Information Governance Department.

2. FairWarning Alerts – issued to line managers.

A report will be issued to you if Fairwarning identifies any suspicious activity performance on the Emergency Care Summary system noted against the pharmacy login details. Any activity which may flag as inappropriate use includes, but is not restricted to, viewing own record or that of a member of their family or other person residing at the same address, a neighbour or a work colleague or patient records from a particular security group. If you, or any member of staff, has a concern about who may have been accessing a particular health record then Information Governance can produce a tailored report to your design.

When you receive this alert, you should check whether there is a legitimate clinical or administrative reason to have accessed these records. If there is, this is known as a False Positive and the reasons for staff accessing the records should be sent to FairWarning@aapct.scot.nhs.uk. Until then the alert will remain active and will be investigated in due course.

If a False Positive has been identified and justification has been received it will be removed from the Fairwarning report and no further action taken.

Where the Fairwarning system has detected a breach of confidentiality, then this will need to be fully investigated by the Information Governance department.

Where it is apparent that the staff member had no legitimate clinical or administrative reason to access the record, then as Pharmacy Manager you should contact Information Governance immediately. An investigation will then be initiated in accordance with NHS Ayrshire & Arran's Information Governance policy. If the data protection breach is serious it may need to be escalated to the Information Commissioners Office. If the data protection breach is deemed serious enough it can lead to prosecution.

Fairwarning does not alter any of the policies of NHS Ayrshire & Arran or existing laws regarding access to patients' health records. Fairwarning simply identifies and highlights instances where system access privileges are suspected of 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 GDPR and Data Protection Act 2018. is a legal requirement and NHS Ayrshire & Arran, in common with all NHS organisations, must be able to demonstrate that non-compliance is dealt with appropriately. For more detailed advice, please contact the Information Governance Department informationgovernance@aapct.scot.nhs.uk