NHS Lanarkshire takes the confidentiality of personal information and its responsibilities under the Data Protection Act very seriously.

Even if with good intentions, staff looking at a clinical record or personal information without authorisation could face disciplinary action.

Protect patients. Protect colleagues. Protect yourself.

- ❖ Visit the Information Assurance pages in the eHealth section of FirstPort for more information on FairWarning and NHS Lanarkshire's information assurance policies:

  http://firstport2/staff-support/ehealth-ict

- ❖ Complete the Safe Information Handling module on LearnPro. This is mandatory training for all staff:

  https://nhs.learnprouk.com

- ❖ Share this leaflet with your colleagues and remind them of the importance of good information assurance practices.

Pub. date:	Nov 2013
Review date:	Nov 2015
Issue No:	01
Department:	

NHS
Lanarkshire

Fair Warning

Closing the loop
On staff who snoop

New monitoring system to automatically spot inappropriate access to electronic patient and staff records

What is FairWarning?

FairWarning is a new monitoring system that will automatically spot inappropriate access to electronic patient and staff records.

It goes live in NHS Lanarkshire on Monday 2 December 2013. Other health boards with FairWarning have identified staff accessing records inappropriately, leading to an increase in disciplinary action.

NHS Lanarkshire staff are being urged to follow information security policies and practices to avoid facing serious consequences.

FairWarning will track NHS Lanarkshire clinical systems in real time and automatically flag up the following confidentiality breaches

Protect patients. Protect colleagues. Protect yourself.

Don't access your own information

Accessing your own records for any purpose using access permissions granted in respect of a job function is not allowed. This includes checking for clinical results, booking clinical appointments or ascertaining CHI numbers. There are established local Subject Access Request procedures to provide employees with access to their records.

Don't access family members' information

Accessing your family's or partner's records for any purpose is not allowed, even if they have given you permission. Accessing your child's record is also not permissible. This includes checking a date of birth so you don't forget a birthday or checking an address so you can send a Christmas card.

Don't access neighbours' information

Accessing neighbours' records, even at their request, is not permitted unless the neighbour is a patient and the employee is directly involved in their treatment. Neighbours can be identified by FairWarning through postcode matching.

Don't access your colleagues' information

Accessing colleagues' records, even at their request, is not permitted unless the colleague is a patient and the you are directly involved in their treatment. This includes checking things like dates of birth, so you can maintain the departmental birthday fund.

Don't access a high profile patient's information

All individuals are entitled to the same level of privacy and confidentiality no matter who they are. Certain individuals generate a higher level of interest. FairWarning allows all access to their data to be monitored and justification for access to be investigated.

Don't breach when training staff

When demonstrating a clinical system to bank staff or new starts do not use your own record or theirs. Show them the system using the next patient being seen to ensure appropriate access. Where a system has a training module, this should always be used in the first instance.

Avoid other inappropriate access

Large numbers of records being accessed over a relatively short period of time could indicate casual browsing, which will be flagged by FairWarning. An example of behavior to avoid is checking addresses of members of a dance class that you run. Regular accesses with the same username over a 24-hour period could indicate password sharing. As with all highlighted potential breaches this would be fully investigated. Staff should not share their password and log-in details with colleagues. You are ultimately responsible for any unauthorised access using your details.