Northern Ireland Ambulance Service
Health and Social Care Trust

CALDICOTT PRINICPLES

CALDICOTT, CONFIDENTIALITY AND DATA PROTECTION

GUIDANCE ON HOW CALDICOTT PRINCIPLES RELATE TO STAFF AND SERVICE USERS

This guidance has been developed to support and provide additional guidelines to staff and service users on the Northern Ireland Ambulance Service Health and Social Care Trust's (NIAS) commitment to information security and confidentiality.

What is 'Caldicott'?

Back in 1997, a review was carried out by the Caldicott Committee to investigate ways in which service user information is used within the National Health Service (NHS) (Health and Social Care in Northern Ireland). The aim was to improve the quality of, and protect service user information ie information about patients. The investigation identified certain principles that NHS organisations should adopt and which are known as the Caldicott principles (the investigation was Chaired by Dame Fiona Caldicott)

As part of the recommendations NHS bodies were tasked with identifying a senior Director to take responsibility and act as the 'Caldicott Guardian'.

Who is the Caldicott Guardian?

The NIAS Trust's Caldicott Guardian is currently Doctor David McManus, Executive Medical Director who is based at Trust Headquarters, Site 30, Knockbracken Healthcare Park, Saintfield Road, Belfast, BT8 8SG.

What does he do?

The Caldicott Guardian ensures that high standards of patient and personal information security and confidentiality are implemented throughout the Trust. The Caldicott Guardian ensures that confidentiality is a Trust priority and relevant issues are presented at Board level.

Adoption of Caldicott Principles

NIAS is committed to implementing the recommendations of the Caldicott Committee's Report on the Review of Patient Identifiable Information.

The report is based on six principles which ask us, when using patient identifiable information to:

1. **Justify the purpose;**
2. **Use only when necessary;**
3. **Use the minimum necessary;**
4. **Access on a 'need to know basis';**
5. **Be aware of your responsibilities;**
6. **Understand and comply with the law.**

1. **Justify the Purpose**

There are three basic rules for making a lawful disclosure of patient confidential information:

- Where a person to whom the information relates has consented;
- Where disclosure is in the public interest;
- Where there is a legal duty to do so e.g Court Order

2. **Use only when Necessary**

Staff must obtain awareness of the systems and processes currently in place that ensure personal information is not inappropriately disclosed, for example adopting safe procedures for answering telephone queries, the use of fax machines and information sharing protocols that set out the terms on which personal information may be shared with an external organisation.

Guidance must also be observed on the avoidance of inadvertent disclosure caused by discussion of patient details in inappropriate venues, e.g. the canteen, in the lift, in a vehicle when transporting other patients, in a rest room etc.

When exchanging information, particularly with other organisations through electronic communications, information should normally be be "anonymised". For example, rather than using a person's full name and other information that could easily identify them, using their Health and Social Care number is a good practice.

By taking personal information out of communications (wherever possible) we reduce the risk of breaches of confidentiality.

Confidential information, especially patient information, should never be sent via email to any Internet based e-mail address without valid encryption or passwords in place. The Internet is not considered a secure "zone".

3. **Use the Minimum Necessary**

Staff should be made aware that even where there is a genuine reason to disclose personal information this will not often require the whole of a patient's record to be disclosed. In order to reduce the risk of data loss or breaches of confidentiality, try not to use excessive amounts of information. Don't make a patient's entire case history available to someone who only needs a particular snippet of information from it.

4. **Access on a 'Need to Know Basis'**

Always take care not to let sensitive information fall into the wrong hands. People, who ask for information such as Solicitors, other HSCS organisations, or even the Police, are not always legally entitled to access it.

It's also worth taking extra care when saving information on a computer system. Putting computer files into incorrect places on the system may mean that unauthorised people may be able to access sensitive information. When using electronic clinical care records it is essential that passwords are not shared and that staff log out of the system if they leave their computer unattended.

5. **Be aware of your Responsibilities**

Simply being aware of the fundamental need for confidentiality, integrity and availability of information will help you make the right decisions.

Ensure that you are familiar with Trust's Policies e.g Code of Practice on Confidentiality of Service User Information, Data Protection Policy etc There are also specific clauses in your employment contract relating to confidentiality.

6. **Understand and Comply with the Law**

Thankfully not everyone is expected to be an expert in information law. Most of the time it's likely that the information you work with will be within established procedures or within the defined scope of information systems. However from time to time you may find that a particular task means you have to use or exchange information in a way that you haven't done before, that may not fit anywhere within established procedures. In such a situation it is always best to check with secondary guidance via your Line manager if in doubt around any legal implications or other information security risk.

Trust Contacts:

Doctor David McManus
Caldicott Guardian
Email: david.mcmanus@nias.hscni.net

Doctor Nigel Ruddell
Deputy Caldicott Guardian
Email: nigel.ruddell@nias.hscni.net

Sharon McCue
Senior Information Risk Owner/Executive Director of Finance
Email: sharon.mccue@nias.hscni.net

Alison Vitty
Information Governance Lead
Email: alison.vitty@nias.hscni.net

The Trust has a range of policies and procedures to support compliance with Caldicott principles and these are placed on the Trust's Intranet/