Appendix 12 to
DUNCAN'S Minibus
Policy
& Code of Practice for
the Safe Use of
Minibuses
Dated: 20 Feb 2023

Duncan Private Hire Code of Conduct Policy

Background

All NHS organisations work to a Code of Conduct for handling patient/client-identifiable information. Working to the same Code of Conduct will help ensure a more unified approach across the organisations to the way Duncan's handle, store, transfer and work with patient/client information. This also helps ensure compliance with the Data Protection Act 1998.

The Health Service holds large amounts of confidential information about you, members of your family, friends, and colleagues; but the vast majority of this information will be about strangers, most of whom you are unlikely to meet. This information is classed as patient/client-Identifiable information. The information belongs to the patient/clients. Their information should be treated with as much respect and integrity as you would like others to treat your own information. It is your responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that patient/client-identifiable information is not made available to unauthorised persons.

This Code of Conduct on confidentiality, which is mandatory for all organisations, aims to clarify the principles that govern all use of patient/client-identifiable information and to ensure that certain practices are adhered to. None of these practices is onerous and they should already be in everyday use. This document restates them as an expectation of how systems should be maintained.

The Code of Conduct is about promoting best practice and continuing improvement in the use of personal health information as an integral part of patient/client care. Involving patient/clients in decisions about their healthcare information and how it is used is also integral to improving patient/client confidence in their health services
Protection of personal health information is part of good practice and is underpinned by the common law duty of confidentiality, the implementation of the Data Protection Act 1998, Codes of Professional Practice, and the Human Rights Act 1998.

Breaches of confidentiality are a serious matter. Non-compliance with this code may result in disciplinary action being taken. No employee shall knowingly misuse any information or allow others to do so. Careless or deliberate misuse of patient/client-identifiable information may result in that organisation, and in some cases the individual concerned, being prosecuted.

Aim of The Document

This document seeks to provide a code of conduct for all staff, which will ensure the confidentiality of patient/client-identifiable information at all times.

Scope

The code relates only to patient/client-identifiable information as defined within the Data Protection Act 1998.

Disciplinary and Legal Implications

Generally, there are four main areas of law which constrain the use and disclosure of confidential information. These are briefly described below:

The Data Protection Act 1998 (DPA)

The DPA is designed to control the use, storage and processing of personal data in whatever format - especially where there is a risk to personal privacy. Patient/clients and staff should be aware that their information will be stored and processed on a computer/PDA.

Common Law of Confidentiality

Although not written in statute, the principle of the common law of confidentiality states that information confided should not be used or disclosed further, except as originally understood by the confider or with her/his subsequent permission. In other words, if you are told something in confidence, you are not at liberty to disclose the information without permission.

Human Rights Act 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Administrative Law

Administrative law governs the actions of public authorities to ensure that they operate within their lawful powers. In other words, the authority must possess the power to carry out what it intends to do and is particularly relevant to the issue of patient/client consent.

What do you do if in doubt about handling patient/client-identifiable information?

If you are in doubt regarding the handling of patient/client-identifiable information, ask the advice of your manager.

Users' Rights

Patient/clients and families have a right to believe and expect that private and personal information given in confidence will be used for the purposes for which it was originally given, and not released to others without their consent. Everyone in Duncan's must safeguard the integrity and confidentiality of, and access to sensitive information.

Definitions

What is Patient/client-identifiable information?

"All items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patient/clients and hence should be appropriately protected to safeguard confidentiality"

These items include:

Surname	Forename
Initials	Address
Date of birth	Other dates (e.g. death, diagnosis)
Postcode	Occupation
Sex	NHS number
National Insurance number	Ethnic group

Local identifier (e.g. hospital or GP practice number)

or a combination of these pieces of information.

Who is an unauthorised person?

Your job role, or level of access to a computer/PDA system/PDA, provides you with a level of authority to access information. Do not assume that all your work colleagues are authorised to see the same information that you are. Even if they are in a more senior role to you - if they do not need to know the information, they do not need to have it. If you are in doubt as to whether you should share the information with one of your colleagues, seek the advice of your manager.

In certain instances, members of staff may have a statutory responsibility to pass on patient/client information.

We have a statutory obligation to notify the government of certain infectious diseases for public health purposes, e.g. measles, mumps, meningitis, tuberculosis, but not HIV/AIDS.

Births and deaths must also be notified.

Limited information is shared with health authorities and public health departments to assist with the organisation of national public health programmes, e.g. breast screening, cervical smear tests and childhood immunisation.

Do not access patient/client information for anything other than your official duties, as misuse will result in disciplinary action. It is not acceptable for staff to access their own records, or those of relatives, friends, or neighbours on their behalf. Staff and patient/clients have rights of access to their own health and personnel records, but this access should only be allowed in accordance with the guidance of the Data Protection Act 1998. Duncan's manager will be able to provide details.

Patient/client/client-identifiable information must not be used in training, testing systems or demonstrations without explicit consent.

What is meant by the transfer of patient/client/client-identifiable information?

The transfer of patient/client-identifiable information, by whatever means, can be as simple as:

- Taking a document and giving it to a colleague
- Making a telephone call
- Sending a fax
- Passing on information held on computer/PDA/PDA, for example confidential clinical information held on patient/client records

In all cases, however simple or complicated, the following principles below, and must be adhered to in order to ensure that patient/client-identifiable information is not disclosed inappropriately.

Principles:

- Justify the purpose
- Don't use patient/client-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient/client-identifiable information
- Access to patient/client-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law

Ensuring Confidentiality

Physical security

Room access – Patient/client-identifiable information should not be left unattended. However, where this can be justified, consideration should be given to restricting room access.

If the room can be locked without compromising patient/client care (e.g. where the patient/client information is unlikely to be needed by non-key-holders), then it should be locked.

Work areas - Identifiable, confidential information should always be held securely. In any area which is not secure, and which can be accessed by a wide range of people (including possibly the public), such information should be put/locked away immediately after it has been finished with. Where it is impractical for this to be achieved, access to the work area must be restricted. Examples of this are:

- Where work is being undertaken simultaneously on samples from a number of patient/clients in a laboratory or clinical area that only laboratory or clinical staff may enter.

- Where reports are dictated on a number of patient/clients seen within a clinic in a reporting/medical office that only medical staff may enter.

- Where a computer/PDA screen is angled to deny unauthorised viewing of confidential data.

Safeguarding information

Never leave patient/client-identifiable information around for others to find.

Wherever possible, avoid taking confidential information away from your work premises. Where this is necessary in order to carry out your duties (e.g. home visit to a patient/client), you must keep the information secure and make every effort to ensure that it does not get misplaced, lost or stolen.

Remember - you are bound by the same rules of confidentiality while away from your place of work as when you are at your desk.

When disposing of paper-based information, ensure that it is shredded. Never put confidential information directly into a general wastepaper bin or recycling bin. If your organisation has a designated confidential waste destruction programme, you must follow the requirements of that programme which can be checked with your head of department. Work diaries can hold a great deal of personal information and should be kept secure when not in use. Precautions should be taken when transporting your work diary to ensure it is in your care at all times.

Do not take personal notes or pocketbooks containing patient/client-identifiable information away from your place of work. If the information is no longer required, it should be disposed of appropriately. If the information is required for an on-going purpose, it should be locked securely away. All personal notes and pocketbooks containing patient/client-identifiable information must be handed back to your manager if you no longer need them for your job.

If documents containing patient/client information come into your possession and you are not the intended recipient, you should either forward these to the named person for action or storage or, if there is no named person, to your manager. If you identify any document containing patient/client information, such as letters or clinical results, you should make every effort to decrease the possibility of these being seen by inappropriate persons by obscuring or turning them over.

Adopt a clear desk policy.

Patient/client-identifiable information left unattended.

Caution should be exercised at all times when working with patient/client-identifiable information.

Only have the minimum information necessary on your desk for you to carry out your work. Any other related information should be put away securely, preferably locked away.

Do not walk away from your work area leaving any documents exposed for unauthorised persons to see.

Information transfer

It is imperative that the utmost care is exercised when transferring patient/client-identifiable information. To this end written documents as well as fax machines and email should be used with care. When internal courier post or public mail is used, it is essential to confirm that the addressee details are correct. The basic rule is that in all circumstances where patient/client-identifiable data is shared, by whatever method, the items transferred should be restricted to a minimum. Only essential items of information should be included. Other items should be omitted or blocked out before transmission.

If transferring paper notes which contain patient/client-identifiable information, make sure “CONFIDENTIAL” is marked in a prominent place on the front of the envelope. Ensure that the address of the recipient is correct and clearly stated, using the following format:

- Name
- designation (job title)
- department
- organisational address

Write a return address on the back of the envelope (if using a plain envelope)

If patient/client-identifiable information is to be sent in carrier (internal) envelopes, the envelope must be sealed and marked “CONFIDENTIAL”. Internal mail should still be properly named and addressed, e.g. not just to "Clark from Peter".

Do not pass documents containing patient/client-identifiable information to other colleagues. Always ensure that patient/client-identifiable information is in a sealed envelope addressed to the recipient and clearly marked “CONFIDENTIAL”.

Transfer between hospital sites, clinics, community bases etc.

You should always ensure that a secure system for transferring care records (or other personal information that identifies individuals) between sites is used.

Only authorised personnel may assist in the transfer of patient/client records where an office, department or practice is moving premises from one site to another. This must be done under the guidance of an authorised employee/employees of that relevant organisation.

Indiscreet conversations

Ensure you cannot be overheard by unauthorised people when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about confidential information. In these situations, if you do not need to identify a patient/client by name, do not do so Consideration needs to be given to the siting of an answer phone to ensure that recorded conversations cannot be overheard or otherwise inappropriately accessed.

During team meetings/briefings staff should bear in mind that they might be overheard by other people in the same room. While it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the patient/client's rights.

It is not appropriate to discuss personal information in hallways, corridors or stairways or any other public place where you might be overheard. When speaking to a patient/client or carer on the telephone, confirm the caller's identity or use ring back. If in doubt, ask.

Safeguarding electronic computer/PDA information

The security and confidentiality of information held on computer/PDA must be maintained at all times.

- Never leave a computer/PDA logged on to a system and unprotected. Always protect the system (e.g. log off or use a password-protected screensaver) when you have finished or stop using it for a period. Always log off when you have finished. Failure to do this not only leads to a risk of unauthorised access to patient/client information, but you will be held responsible for any actions associated with your sign-on
- Do not walk away from your work area and leave patient/client-identifiable information on your screen for unauthorised persons to see. If you need to leave your desk, you should protect the system (e.g. log off or use a password-protected screensaver)
- Where it is necessary for patient/client-identifiable information to be stored on your computer/PDA, ensure that it is stored in a secure way with password protection
- Always remove your Smartcard from your computer/PDA (if using one to access systems) when leaving your workstation

- Do not keep any patient/client-identifiable information longer than necessary. Delete personal files you do not need to keep and if the information is stored on diskette, tape or CD, ensure that it is clearly labelled and locked away. When the information held is no longer required, the diskette, tape, or CD must be reformatted, erased or destroyed. Computer/PDA users should remember that when deleting files, they may be moved to a "recycle bin". Therefore, the recycle bin should be emptied on a regular basis. If in doubt, check
- Passwords are the keys that provide access to information; you must not disclose your network password to anyone under any circumstances. Never write your password down as this could be seen by other users, and always change your password when prompted. It is recommended that passwords should be a minimum of 6 characters and be a mixture of letters and numbers, i.e. using 5 instead of S, 1 instead of I, etc
- Turn off your computer/PDA at the end of the working day unless it is needed to work unattended, e.g. for printouts
- Never use anyone else's code and password, even to be helpful. Never, as a manager, ask anyone to use another's password for convenience. If it is absolutely necessary, (e.g. to access information when a patient/client or other person is in danger and the owner of the password cannot be found), contact your manager

Destruction and /or disposal of computer/PDAs, or parts thereof, must be carried out by your manager. This will ensure that all information is stripped from the computer/PDA and disposed of using the correct procedures. You should not remove or relocate computer/PDAs without first checking with your manager.

If you use a portable computer/PDA outside your place of work, ensure that:

- You have the authority to take equipment off-site
- You have permission to transfer patient/client-identifiable information off site
- Your computer/PDA is password-protected to BIOS level which will be set by the IT department which provides the portable
- You store back-ups securely and complete them regularly whilst using portables.
- Databases are encrypted
- Keep anti-virus software up to date – see the IT department or Systems Manager for assistance if necessary
- All equipment is locked away when not in use
- Every effort is taken to prevent loss or theft of your computer/PDA
- You do not leave your computer/PDA in your car