Confidentiality

Protecting Patient/Person Information

What is Patient Identifiable Information?

- Name
- Address
- Post Code
- Date of Birth
- Gender
- CHI Number

Anything that can be used to identify a patient directly or indirectly.

What is Confidentiality?

All and any information held about a patient in any form is strictly confidential

- Manual: case records, clinic lists, labels, IP/OP scanning folders, etc
- Electronic: All patient information held on all systems i.e. Trak, Clinical Portal, Opera, Emis(mental health) etc
- Verbal communication: Conversations with colleagues re patient, telephone calls i.e. with or about patients etc

Who has access?

- Medical & Nursing staff may have access to a patient’s record if the patient is attending their ward or clinic.
- Admin staff may have access if:
  - Processing patient referrals
  - Making appointments
  - Booking patients in at ED/MIU
  - Admitting Patients
  - Update demographic details

*Police & Managers within the Health Service **DO NOT** have the **automatic** right of access without legitimate purpose or documentation.*

Good Practice: Manual

- Case Records/scanning folders must never be left unattended in public areas
- Any patient demographic information should be protected in pick up areas for nursing staff, reception desks etc.
- Areas which require to be unstaffed should be locked/alarmed e.g. medical records in a separate building

Good Practice: Electronic

- Never reveal your password to anyone or allow anyone to use your password
- Ensure patients are unable to view patient information on computer screens
- If leaving your PC, even if only for a few moments, LOG OFF or lock your computer, e.g. control-alt-delete or windows-L
- Ensure patient records on screen are never left unattended

Good Practice: Verbal

- Never discuss patient identifiable information in an area where it can be over heard e.g. Outpatients, on the bus, in the canteen.

- Never discuss patient details with anyone who is not involved in the care of the patient or whose role does not require that information.

Good Practice: Verbal continued…

- On receipt of a telephone call while dealing with a patient at the reception desk, staff **MUST** use the silent button on the telephone to ensure that the person on the telephone does not overhear the patient at the desk giving personal information or vice versa.
- Ask the patient to confirm their details, we do not supply details to the patient. By the patient confirming the details to us , this is them giving consent.

Good Practice: Verbal continued…

- Never ask a friend or relative who is attending why they are here today - they may not wish to discuss why they are attending hospital.
- If they engage in a conversation and volunteer information, you should wish them well but should not discuss with anyone.

Fax Machines

- Previously, one of the most common breaches of confidentiality occurs when documents containing patient identifiable information were sent by fax machines.
- Fax machines should only be used when there are no other contact methods available and safe haven procedures should be followed

Scanning Documents

- The use of scanning documents to be sent as email attachments is more common now than fax machines
- When scanning documents to be sent as email attachment to recipient, always ensure you are sending to correct person
- The safest way of doing this is to store frequent users email addresses in scanning machine, and to scan documents to yourself so they can be checked and then forwarded from your email account

Examples of breaches of confidentiality include:

Social Media

Social Media e.g. Facebook, Twitter, Instagram, Snapchat etc

- Posting a conversation you have had with a patient or posting photographs/images of patients on social networking sites such as Facebook.
- Posting any information that may identify a patient or a situation that has occurred within the hospital on social networking sites.

Scenarios

- An elderly lady collapses at the reception desk you are working at and you think nothing of it and say later that night on Facebook "guess what happened today at work a lady collapsed in front of me“. One of your friends could like your comment and one of their friends could be related and say “that’s my gran”. Situations that happen in work should never be discussed on social media.
- On your profile you state you work for a specific hospital/NHS and you post a viewpoint on a subject, this could be perceived as the NHS viewpoint
- Checking in on Facebook that you are at your place of work

Social Media e.g. Facebook, Twitter, Instagram, Snapchat etc continued……

- A member of staff may have been off on holiday or sick leave, you take a photo of their desk with lots of work on it "saying look what you have to come back to". Pictures can be zoomed/enhanced to show patient information i.e. CHI, name etc
- You discuss a colleague on Facebook and someone on your friends list likes it; they may be a friend of the person you are discussing
- Using social media in working hours isn't permitted; for further information on this please see the policy on Personal Use of Social Media on StaffNet.

Other examples of breaches of confidentiality include:

- Mentioning to family or friends that you saw a mutual friend at an outpatient appointment

- Using hospital systems or health records to check whether a friend or colleague is attending

- Using hospital systems or health records to check a friend or colleagues address or phone number.

Other examples of breaches of confidentiality continued…

- Divulging the contents of a patients tests or other clinical information to anyone who is not involved in the care of the patient or whose role does not require that information.

- Reading a case record/scanning folder or accessing patient information systems for information belonging to someone you know when you do not have to do this as part of your job; this includes accessing your own information or record.

- Accessing clinical information when your role does not require you to do so.

Fairwarning

FairWarning® was introduced on Monday 1St October 2018

- It is a new monitoring system which detects potential instances of unauthorised access to patient information held within electronic information systems and tracks access in real time.
- We know the vast majority of staff respect confidentiality and that unauthorised access to patient information is rare. However, FairWarning is an opportunity to provide an even higher level of assurance that patient information is safe with us.

FairWarning: continued

- Staff who have access to patient identifiable information are being urged to know their responsibilities with regard to confidentiality ahead of the introduction of FairWarning.
- We have produced guidance for both staff and managers. To access this click on link provided by your Line Manager or Core Brief which has been sent.
- For further information on patient confidentiality and the FairWarning system, please contact the Information Governance Team at Data.Protection@ggc.scot.nhs.uk

Inbound calls-Enquiries

- Informing a relative of a patients discharge details once the patient has been discharged from ward/ED

- If relatives call regarding a patient and the patient has already been discharged they should be told "The patient is not currently an inpatient"

- If relatives call looking for an update on ED/MIU attendance and the patient has been discharged they should be told "The patient is not currently in the hospital"

Inbound calls-Enquiries continued…

- Current Inpatient
- Informing a relative of a patients appointment.
- PFB/OPT IN calls.

OUTBOUND CALLS

- If phoning patients to offer/cancel an appointment we would always ask to speak to the patient. If a relative etc answers the phone and asks who is calling we would give our name and advise that we are calling from GGC. If the relative etc asks what the call is relating to our staff would ask the relative when the patient will be back home to allow us to call back - a name and number can be left. If the patient will not be able to return the call then a message can be left with the relative.
- Answer machine messages shouldn't be left under normal circumstances however there is recognition that on some occasions this is necessary.
- However there maybe some occasions when the person cannot speak English/has hearing problems/has dementia etc and the relative is their carer and we would make a judgement call especially if cancelling a short notice appointment

ALERTS

- Before giving out appointment information, wards etc always check alerts in Patient Activity screen.

- Only alerts health records staff are allowed to add are:

  - Turning off Netcall Reminder Calls
  - Interpreter Alerts

Security

- ID badges must be worn at all times
- Uniform to be worn as per Uniform Policy
- Staff must be aware of the need for security and their areas of responsibility
- Staff should be aware of their surroundings and report anything untoward

Fraud

- In NHS Greater Glasgow and Clyde (NHSGGC), we want every member of staff to be aware that Fraud can occur in the NHS and that every penny the Board loses to fraud is a penny that is not available to spend on patient care. It is the duty of every staff member to comply with the Board's Code of Conduct for Staff and **Fraud Policy** , and to report any suspicions of fraud immediately. If you think that fraud has occurred, or is about to occur, you should report details to your manager, who will raise the matter with the Fraud Liaison Officer (FLO) and Human Resources (HR).

Any breach or suspected breach of security should be reported to an employee’s line manager

Breach of confidentiality is a serious offence and can lead to dismissal

Questions?