Barts Health NHS
NHS Trust

INFORMATION GOVERNANCE CODE OF CONDUCT

Barts Health NHS Trust takes information security seriously. As a member of staff, you must be aware of your responsibilities when handling confidential information.

Information is essential to provide safe and quality care for patients and to manage our services and resources. In order to successfully deliver highest quality services, we must manage information securely, efficiently and effectively, based on robust policies, procedures, management accountability and a sound governance framework for information management.

Confidential information can include anything that relates to individuals (e.g. health records, complaints, and serious untoward incidents), held either on paper or electronically. It is a legal duty of all staff to ensure that confidentiality is maintained when they are handling personal or sensitive information.

There are many ways in which confidentiality could be breached; a few examples include:

- *Accessing records you have no legitimate reason to see, for example your own, your relatives and friends health records, even with their consent (unless it is within your job role to deal with such requests).*
- *Displaying or leaving records open, unattended or insecure.*
- *Giving out information over the telephone, by fax or email to inappropriate people.*
- *Holding conversations about individuals where others could overhear.*

1. What is Person Identifiable Data (PID)?

- *Name, address, full postcode, date of birth, financial details of patients or staff*
- *Pictures, photographs, videos, audio-tapes or other images of patients; copies of passports, birth certificates of staff*
- *NHS number and local patient identifiable codes; national insurance number or payroll number of staff*
- *Anything else that may be used to identify an individual directly or indirectly. For example, rare diseases, drug treatments or statistical analyses with very small numbers within a small population.*

2. Transferring PID

a. Portable Devices (including laptops, tablets, smartphones, DVDs, CDs, USB flash drives)

- Ensure the whole device is encrypted wherever possible. Contact the ICT Service Desk to arrange.
- Do not open emails/files that include PID on home computers/devices.
- Store only the minimum amount of PID necessary for the current purpose on the device.
- Store PID only for the time period when it is actively being used.
- Delete PID from the device immediately after use.
- Ensure the device is physically secure when unattended.
- While working on a Trust site, use the Trust network rather than a portable device to store data.
- Do not use portable devices for permanent storage of data.
- Any data on the device must be backed up on the Trust network.

b. Post/Courier

- Send PID in a sealed envelope and mark it as “Private and Confidential”.
- The envelope must display the recipient’s name, job title and full contact details.
- To transfer sensitive or bulk data, use Special Delivery post or a courier.
- If using a courier, ensure the Trust has a contract with the courier company.
- Include a return name and address on the back of the envelope.

c. Manual Transfer

- Do not leave PID or portable devices in insecure areas, and use lockable rooms and storage facilities where available.
- Take extra care of PID or portable devices when in busy public places.
- Carry PID and portable devices in protective anonymous bags or cases (i.e. without NHS logo or laptop manufacturer).
- When travelling, ensure that PID and portable devices are stored securely out of sight, but avoid placing them in locations where they could be easily forgotten e.g. overhead racks.
- When travelling by car, ensure PID and portable devices are locked in the boot, but not left in the boot overnight.
- Using PID or portable devices in public could lead to the unauthorised disclosure of data.

d. Email

- When emailing within the organisation ensure PID is sent between Trust accounts:
  @bartshealth.nhs.uk ⇨ @bartshealth.nhs.uk
- When emailing outside the organisation ensure that PID is sent between NHSmail (nhs.net)accounts:
  @NHS.Net ⇨ @NHS.Net
- NHSmail accounts can be requested from the ICT Service Desk. ICT Service Desk can also set up NHSmail accounts for people in external organisations.
- Do not use patient or staff names as an email subject.
- Password protect and encrypt PID using WinZip, where possible.
- Do not use personal email accounts (e.g. Hotmail, Yahoo, gmail) to send or receive PID.
- All bulk transfers of PID should be approved by the IG Team before commencement, then sent via Secure File Transfer.

e. *Telephone*

- Disclosure of PID via telephone should be the exception rather than standard practice.
- Always confirm the identity of the other party before disclosing information.
- Dial back arrangements should be used to ascertain the person is authorised to receive the data; the dial back should be done through the callers' switchboard number rather than a direct line.
- The member of staff should ensure that they know the reason why the other party requires the information.
- Recorded telephone messages must be received into a secured, password protected voicemail box.
- For times of absence, a deputy should be appointed and an administrator password made available.
- Any log books used to record phone messages should be stored securely.

f. Fax

- When faxing PID, a safe haven fax procedures should be followed:
  - A cover sheet should be used and state who the recipient is and be marked "for the attention of the addressee only & Private and Confidential".
  - Anonymise PID wherever possible. If this is not possible, restrict to the minimum necessary for the purpose of the disclosure e.g. use NHS number instead of name, DoB etc.
  - Telephone the recipient of the fax to let them know you are sending them PID.
  - Always double check the fax number before you hit the Send button.
  - Request a report sheet to confirm that the transmission was successful.
  - If necessary, contact the recipient to ensure they have received the fax.
  - Never leave the fax machine unattended whilst the fax is being transmitted.
  - Safe haven fax machines must be located in a secure office which is always locked when not in use/occupied.
- All faxes must be to a named individual and are dealt in a timely fashion.

3. *Logins and Passwords*

- When using a computer or laptop:
  - Always lock (**CTRL+ALT+DEL**) your computer or laptop when you leave your desk.
  - Never share individual login details and passwords with other colleagues.

4. *Records Management*

- Do not store confidential Trust data on the C: drive or Desktop.
- Use a secure/restricted shared drive, your H: drive (for non-work related files), or approved Trust software (e.g. Datix, Sharepoint, etc).
- When not in use, always lock paper-based information securely away.
- Emails containing PID must be filed appropriately on receipt, e.g. in the health record or staff file, and then deleted from the mailbox.
- Information should be disposed of in accordance with the Trust Records Retention and Disposal policy, and only in confidential waste bins.

5. *Sharing Information Verbally*

- Take care to ensure that your conversation cannot be overheard by others who do not need to know.

6. *Social Networking and Blogging*

- You must not upload work related content to a social networking or blogging account.

7. *Incident Reporting*

- Information Governance incidents (e.g. loss of information, breaches of confidentiality) must be reported in line with Trust policy and immediately to the Information Governance Manager.

8. *Freedom of Information (FoI) Act Requests*

- Requests can be made to any member of staff; all staff have a legal duty to assist requesters.
- Direct reference the FoI Act does not need to be included in the request for it to be considered as such.
- Requests must be made in a letter or email, giving the requesters' name and address.
- The Trust must respond within 20 working days.
- If you receive a request, please immediately contact the FOI Co-ordinator.

9. *More Information*

Further information is available from:

- Data Protection Policy
- Information Security Policy
- Information Governance Policy
- Confidentiality Code of Practice
- Retention & Disposal Policy
- Freedom of Information Policy
- FAQs on Trust Intranet

For advice and guidance please contact the **Information Governance** team:

Telephone	14–46028/7 (020 3594 6028/7)
Email	informationgovernance@bartshealth.nhs.uk
Intranet	http://bartshealthintranet/About-Us/Corporate-Directorates/Corporate-Affairs/Information-Governance/Index.aspx

Or the **Records Management** team:

Telephone	18-4866 or 18-4361 (020 7480 4866/4361)
Email	recordsmanagement@bartshealth.nhs.uk foi@bartshealth.nhs.uk
Intranet	http://bartshealthintranet/About-Us/Corporate-Directorates/Corporate-Affairs/Records-Management/Index.aspx http://bartshealthintranet/About-Us/Corporate-Directorates/Corporate-Affairs/Records-Management/Freedom-of-Information.aspx

---

By completing the Information Governance quiz you are confirming that you have also reviewed this Code of Conduct document. Failure to comply with these guidelines and Trust Policies may lead to disciplinary action taken against staff.