**Clinical Confidentiality Form**

**&**

**Information Governance Code of Conduct Form**

**Please complete the following two forms below.**

**Please bring the completed signed forms to your Pre-Employment meeting at:**

**Barts Health NHS Trust**

**20 Churchill Place,
Canary Wharf,**

**London,
E14 5HJ**

**Guidelines on Clinical Confidentiality**

Introduction:

This document is a summary of the Trust’s guidelines on Clinical Confidentiality (Policy No: RHT/POL/006/OPS) and relates to clinical information on patients, and includes the limited circumstances when a patient’s details may be disclosed. This summary is based on existing guidelines approved by the GMC, NMC, recent consultation with Caldicott Committee, and complements existing Trust policies. Confidentiality is not only an ethical duty but, is also a legal and contractual obligation.

Application:

Personal health information is confidential to those involved in the patient’s care. It may not be disclosed to others without the consent and permission of the patient, except in defined exceptional circumstances.

No information may be provided about a competent adult without the patient’s permission – even to relatives. Staff should always seek the patient’s permission at an early stage. In the case of someone who is not competent (e.g. unconscious) it may be helpful to obtain personal and medical information from significant others (e.g. close family); and it is possible to convey the patient’s current status without revealing confidential information.

Particular procedures apply to children. Children under the age of 16 who are able to fully understand (‘Gillick Competence’) the nature and purpose of the information to be disclosed should be treated as adults. Otherwise information can be given to those with parental responsibility and further disclosures to others could be agreed by them where it is in the child’s best interests. It would, however, be good practice to obtain a child’s view where appropriate.

Be careful of unintentional disclosure, e.g. through overhead conversations (within the Trust or outside), telephone calls, written material (especially case notes), and through access to data held on computer. Passwords on the hospital information system (PAS) should not be shared.

Be especially careful of disclosures to the media.

Remember that the duty of confidentiality continues after a patient’s death.

Exceptional Circumstances:

Exceptional Circumstances where disclosures are permitted are set out in the GMC guidance and relate to particular situations:

• When it is in the patient’s best interest, e.g. the patient is believed to be a victim of neglect, or of physical or sexual abuse.

• When it is in the interest of others where there is a risk of death or serious harm, e.g. a patient driving against medical advice

• When there is a statutory duty, e.g. notifiable diseases – when required to do so by a Court

Order.

Management and Contracting Information:

Some information about clinical matters may be necessary for management and contracting purposes, both within the Trust and with outside bodies such as a local health authority. In most instances, unique personal indentifiers, but not the patient’s identity are used. While the information often relates to broad clinical categories, it must be recognised that such information is confidential. For further information please refer to the Caldicott Report which provides a useful framework.

Conclusion:

Clinical Confidentiality is concerned with protecting a patient’s ethical and legal rights and it is your responsibility to ensure that all measures are taken to support the Trust’s policy on confidentiality. Any person who discloses confidential patient information must be prepared to explain and justify such a decision.

First Name: ………….….…………..…… Surname: …..…………………………………….. Signed…………………………………………….…………. Date ………………………….

Barts Health NHS Trust: Newham Hospital, Mile End hospital, , The Royal London Hospital, St Bartholomew’s Hospital and Whipps Cross Hospital.

**Information Governance Code of Conduct**

Barts Health **NHS Trust** takes information security seriously and ensures that staff are aware of their responsibilities when handling all information that should be kept confidential.

Information is required to look after patients and manage services and resources. It is also important for:

* Clinical governance (corporate accountability for clinical performance)
* Corporate governance (meeting standards of accountability and integrity)
* Service planning and performance management.

We must manage information securely, efficiently and effectively, so we need suitable policies, procedures and management accountability to create a sound governance framework for information management.

***All staff are required to read and sign this document***

**Confidential information can be anything that relates to patients (e.g. health records, complaints, and serious untoward incidents), staff or any other person, held either on paper or electronically. Confidentiality is a general legal requirement that applies to all Trust staff when handling personal information about others as part of their job.**

|  |
| --- |
| There are many ways in which confidentiality could be breached, a few are listed below; * Accessing records you have no legitimate reason to see, for example your relatives and friends health records, even with their consent (unless it is within you job role to deal with such requests) – this includes your own patient data which is accessible via a formal subject access request.
* Displaying information in a way that unauthorised people could see items;
	+ Leaving workstations unlocked;
	+ Leaving records open, unattended or insecure;
* Confidential Information disposed of inappropriately;
* Giving out confidential information in person, over the telephone, by fax or email to unauthorised people;
* Holding conversations about individuals where others could overhear.
 |

***Failure to comply with these guidelines and Trust policy may lead to disciplinary action taken against staff.***

1. ***Transfer of Person Identifiable Data (PID)****[[1]](#footnote-1)*
2. ***Portable Devices[[2]](#footnote-2)***

Portable devices should be used as transitional tools for PID only when absolutely necessary for work purposes. The use of any of these items will constitute a risk as they are highly susceptible to loss.

|  |
| --- |
| * Ensure the whole device is encrypted wherever possible. Contact the ICT Service Desk to arrange.
* 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 should be backed up on the Trust network.
 |

1. ***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 (tracked) post or a courier.
* If using a courier, ensure the Trust has a contract with the courier company.
* Include a return name and address in the top left hand corner on the back of the envelope.
 |

1. ***Email***

|  |
| --- |
| a. Do not use personal email accounts (eg. Hotmail) to send or receive PID. b. Always follow NHS Mail policies and guidance for use of email and transfer of PID via email. c. Ensure that you have identified the correct recipient when emailing, being aware that NHS Mail is a national email system, and individuals may have a number in addition to their name. d. Ensure that a patient has consented to receive PID via email before sending it.  |

1. ***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 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.
 |

1. ***Fax***

It should no longer be necessary to use fax in the Trust. If necessary to fax PID, a safe haven fax[[3]](#footnote-3) must be used. If you are unsure whether the machine you are using is a safe haven fax or not, use the following procedures:

|  |
| --- |
| * Anonymise PID wherever possible. If this is not possible, 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.
* The cover sheet should state who the information is for, and be marked "Private and Confidential".
* 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.
 |

1. ***Records Management***

|  |
| --- |
| * Do not store confidential Trust data on the C:drive or Desktop; use a secure/restricted shared drive folder, your H: drive (where appropriate), 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.
 |

1. ***Laptops***

All Trust laptops should be encrypted, and the guidelines for portable devices apply (see section 1a). PID must not be stored on a laptop unless absolutely necessary for work purposes, and good practice guidelines for securing your laptop are as follows:

|  |
| --- |
| * When using a laptop to store PID:
* Always lock it (**CTRL+ALT+DEL**) when you leave your desk.
* When you are transporting or not using the device, make sure it is switched off.
* Do not leave laptops in insecure areas, and use lockable rooms and storage facilities where available.
* Take extra care of laptops used or transported in busy public places.
* Carry laptops in protective anonymous bags or cases (i.e. without manufacturer logos).
* When travelling, ensure that laptops 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 laptops are locked in the boot, but not left in the boot overnight.
* Use of laptops in public could lead to the unauthorised disclosure of data viewed on the screen.
 |

1. ***More Information***

Further information is available as follows:

|  |  |
| --- | --- |
| * Data Protection Policy
* Information Security Policy
* Information Governance Policy
* Confidentiality Code of Practice
 | * Retention & Disposal Policy
* Email Policy
* Freedom of Information Policy
* Information Governance Quick Reference Guide
* FAQs on Trust Intranet
 |

For advice and guidance contact the Information Governance team:

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

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

I have read and understood the above information and will handle confidential information in line with Trust Policy, GDPR, the Data Protection Act 2018, the common law duty of confidentiality and the Freedom of Information Act 2000. Failure to comply with these guidelines and Trust policy may lead to disciplinary action being taken against me.

**Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signed \_\_­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Department \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***Please sign and return to People Services.***

1. Person-identifiable data (PID) covers patient or staff information, and can include the following:

	* 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. [↑](#footnote-ref-1)
2. Portable devices can include tapes, floppy discs, laptops & handheld computers, Blackberries, iPads, i-phones, optical discs (DVD / CD), solid state memory cards and memory sticks. [↑](#footnote-ref-2)
3. Safe haven faxes are faxes located in a secure office which is always locked when not in use/occupied and all received faxes are to a named individual and are dealt in a timely fashion. [↑](#footnote-ref-3)