Ashford and St. Peter's Hospitals NHS
NHS Foundation Trust

Non ASPH Trust Staff - DATA ACCESS REQUEST – Page 1/3

Please ensure that **all THREE pages** of this contract are returned to:

Information Governance Manager, Health Informatics, Chertsey House, St Peter's Hospital, Chertsey, KT16 0PZ

All fields of this form need to be completed in black ink and BLOCK CAPITALS. Failure to do so could delay access being granted

EMPLOYEE'S DETAILS	
Name of EMPLOYEE:	
Employee's Job Title:	
State Reason for Data Access:	
Employee organisation or agency eg GP practice :	
Employee organisation or agency work address:	
Placement Department within ASPH (if applicable)**:**	
Date of commencement of employment:	
Type of employment: (please tick)	**Temporary:** ☐ **Permanent :** ☐
End Date (if temporary staff)**:**	
Email address: ☐	
Contact Number: ☐	

ASPH Trust Access (Staff based at Ashford or St Peters only)		Community Access (Any individuals requiring access not based on site)	
ASPH email Account	☐	**GP Browser**	☐
Network Account	☐	**Pathology Results** (WinPath Ward Enquirer):	☐
PACS (Centricity Web):	☐	**PACS** (Centricity Web):	☐
PAS (Clinicom):	☐	**PAS** (Clinicom):	☐
Pathology Results (WinPath Ward Enquirer):	☐		
InPatient Lists	☐	*Data Protection Act 1998 : The Trust is registered with the DPA 1998 and your details will be kept secure and used only in connection with access to our Information Systems*	
A&E Tracker	☐		
OnTake Tracker	☐		
Other:	☐		

Ashford and St. Peter's Hospitals NHS
NHS Foundation Trust

Non ASPH Trust Staff - DATA ACCESS REQUEST – Page 2/3

Name of EMPLOYEE:	(BLOCK CAPITALS)

PROFESSIONAL AND PERSONAL IDENTITY CHECKS

TO BE COMPLETED BY REPORTING LINE MANAGER (ASPH or Community)

Please confirm that you have carried out all appropriate vetting checks which are - CRB, Professional Registration, ID checks, two references.

Vetting Completed	YES ☐	NO ☐

Please confirm completion of Information Governance Training (either on-line or face-to-face with an assessment). Evidence of current training (annual) should be attached to this form.

We are unable to provide access to our systems without this requirement being complied with.

Information Governance Training completed, certificate attached.	YES ☐	NO ☐

Line Managers' Details

Line Manager's Name:	
Job Title:	
Work email address:	
Work telephone number:	
Line Managers' Signature confirming above checks: **Date:**	

ASPH Office Only: Ashford & St Peter's Approval**:**			
IG Approval	**Signature:**	**Date:**	**Comments:**
Minerva	**Name:**	**Date on tracker:**	

Ashford and St. Peter's Hospitals NHS
NHS Foundation Trust

Non ASPH Trust Staff - DATA ACCESS REQUEST – Page 3/3

CERTIFICATE OF CONFIDENTIALITY

(to be completed by each individual requesting access)

Your personal responsibility concerning security and confidentiality of information (relating to patients, staff and the organisation)

During the course of your work you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of the Trust. This condition applies during your relationship with the Trust and after the relationship ceases.

Confidential information includes all information relating to the Trust and its patients and employees. Such information may relate to patient records, telephone enquiries about patients or staff, electronic databases or methods of communication, use of fax machines, hand-written notes containing patient information etc. If you are in doubt as to what information may be disclosed, you should check with a manager.

The Data Protection Act 1998 regulates the use of computerised information and paper records of identifiable individuals (patients and staff). The Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal action.

I understand that I am bound by a duty of confidentiality and have read the Confidentiality Code of Conduct. I agree to adhere to this Code of Conduct and the requirements of the Data Protection Act 1998.

EMPLOYEE'S NAME (print):	
SIGNATURE:	
DATE:	
LINE MANAGER'S NAME:	
SIGNATURE:	
DATE:	

Please return completed Honorary Contract (THREE pages) to:
Information Governance Manager, Health Informatics, Chertsey House, St Peter's Hospital, Chertsey, KT16 0PZ

Ashford and St. Peter's Hospitals NHS
NHS Foundation Trust

Process for requesting access to information systems for Non ASPH staff members

For staff who are not employed directly by ASPH, access to information systems needs to be requested.

- A Non-ASPH Trust Staff data access request form needs to be completed by the individuals line manager. This could be the Practice manager for those individuals who work in a GP practice or the Requesting Line Manager for Staff who are working on site at ASPH but employed through an agency or PCT etc.

- This form needs to be completed in full as the process will be delayed should any fields be left blank.

- This form can be completed in advance if the line manager is aware of all the details of the individual. Signature of the Certificate of confidentiality by the employee can take place when they attend their training sessions (however the line manager will need to sign the form when completing in order for this to be processed)

- Forward signed forms to Information Governance Manager, Health Informatics Department, Chertsey House, St Peters' Hospital, KT16 0PZ

- Access request will be reviewed and approved should all be in order

- Access request details then relayed to relevant areas for this to be processed and training arranged as needed.

- Individual will then be contacted once access has been granted and will need to attend training as required.

Should individual's employment term extend beyond that which is stated on the request form, it is the Line Managers responsibility to notify the Minerva Centre of a new 'end date' in order to ensure access is not removed and continues accordingly.

Should an individual have signed an access request form previously and is now in a different role or area, this form needs to be completed again in order to ensure that all details are current and up to date.

Should an individual still be in the same role or area and requires additional access to other information systems, a new form is not required, however an email detailing additional access needs to be forwarded to : ITTraining@asph.nhs.uk by the named line manager.

Ashford and St. Peter's Hospitals NHS
NHS Foundation Trust

CODE OF CONDUCT FOR NON-TRUST EMPLOYEES IN RESPECT OF CONFIDENTIALITY

Information Governance Manager, Information Services, Chertsey House, St Peter's Hospital, Guildford Road, Chertsey, Surrey, KT16 0PZ

Ashford and St. Peter's Hospitals NHS
NHS Foundation Trust

CODE OF CONDUCT FOR NON-TRUST EMPLOYEES IN RESPECT OF CONFIDENTIALITY

Please note that this document should be read and understood in conjunction with the following Trust policies:

- Confidentiality Policy
- Email Policy
- Fax Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Security Policy
- Internet Usage Policy
- Policy for Handling Press Enquiries
- Records Management Policy
- Standards for Practice and Care

If there is anything that is not clear please contact your Manager

1. Purpose of the Code

1.1 All individuals working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and, in addition, for health and other professionals through their own profession's Code/s of Conduct.

1.2 This means that individuals are obliged to keep any person identifiable information strictly confidential e.g. patient and employee records. It should be noted that individuals may also come into contact with non-person identifiable information which should be treated with the same degree of care e.g. business in confidence information such as waiting list data, financial information etc.

1.3 Disclosures and sharing of person identifiable information is governed by the requirements of Acts of Parliament and government guidelines.

1.4 The principle behind this Code of Practice (Code) is that no individual shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.

1.5 This Code has been written to meet the requirements of:

The Data Protection Act 1998
The Human Rights Act 1998
The Computer Misuse Act 1990
The Copyright Designs and Patents Act

This Code has been produced to protect individuals by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

2. Detailed Provisions

2.1 Confidentiality of Information

All individuals are responsible for maintaining the confidentiality of information gained during the course of their work.

2.2 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

For example, information may be held on paper, floppy disc, CD, computer file or printout, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras.

It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any Trust confidential information.

Person identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

During your duty of work you should consider all information to be sensitive, even something such as a patient's name and address. The same standards should be applied to all information you come into contact with.

2.3 **Requests for Information on Patients**

Never give out information on patients or staff to persons who do not "need to know" in order to provide healthcare and treatment.

All requests for identifiable information should be on a justified need and some may also need to be agreed by the Trust's Caldicott Guardian.

Any exceptions to this rule may require you to get written consent from the patient in advance. If the patient is unconscious and unable to give consent, consult with the health professional in charge of the patient's care.

If you have any concerns about disclosing/sharing patient information you must discuss with your manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with you should take down the caller's details and ring them back when you are satisfied the disclosure of information can take place.

2.4 **Telephone Enquiries**

If a request for information is made by telephone,

Always try to check the identity of the caller and check whether they are entitled to the information they request

Take a number, verify it independently and call back if necessary

Remember that even the fact that a patient is in hospital, is confidential. If in doubt consult your manager.

2.5 **Disclosure of Information to Other Employees of the Organisation**

Information on patients should only be released on a need-to-know basis.

Always check the member of staff is who they say they are.

This can be achieved by checking the employee's ID badge and/or their internal extension number or bleep number prior to giving them any information.

If possible also check whether they are entitled to the information.

2.6 **Abuse of Privilege**

It is strictly forbidden for individuals to look at any information relating to their own family, friends, acquaintances or colleagues unless they are directly involved in the patient's clinical care or with the employee's administration on behalf of the Trust. **Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.**

If you have concerns about this issue please discuss with your line manager

2.7 **Carelessness**

Do not talk about patients in public places or where you can be overheard.

Do not leave any medical records or confidential information lying around unattended.

Make sure that any computer screens, or other displays of information, cannot be seen by the general public.

2.8 **Use of Internal and External Post**

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

External Mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as casenotes, or collections of patient records on paper, floppy disc or other media. These should be sent by Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s).

In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

2.9 **Faxing**

Remove person identifiable data from any faxes unless you are faxing to a known secure and private area (Safe Havens).

Faxes should always be addressed to named recipients.

Always check the number to avoid misdialling and ring the recipient to check that they have received the fax.

If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

2.10 **Storage of Confidential Information**

Paper-based confidential information should always be kept locked away and preferably in a room that is locked, and in some cases alarmed (e.g. GUM records) when unattended, particularly at nights and weekends or when the building/office will be unoccupied for a long period of time. This should be tracked accordingly.

PC-based information should not be saved onto local hard drives or onto removable media, but onto the Trust's network.

2.11 **Disposal of Confidential Information**

When disposing of paper-based person identifiable information or confidential information always use 'Confidential Waste' bins/shredders. Keep the waste in a secure place until it can be collected for secure disposal.

This should be done in line with the records retention schedule as set out in the Records Management Policy

2.12 **Confidentiality of Passwords**

Personal passwords issued to or created by individuals should be regarded as confidential and those passwords must not be communicated to anyone.

Passwords should not be written down.

Passwords should not relate to the employee or the system being accessed.

No individual should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to your line manager and may result in disciplinary action and may also breach the Computer Misuse Act 1990 and/or the Data Protection Act 1998 which could lead to criminal action being taken against you.

2.13 **Emailing Confidential Information**

Please seek advice from your manager if you have the need, or possible need, to e-mail patient identifiable information.

Patient identifiers should be removed wherever possible, and only the minimum necessary information sent, this may be considered to be the NHS number but no name or address. This in itself can pose problems as the wrong number may be typed.

Special care should be taken to ensure the information is sent only to recipients who have a "need to know"; always double check you are sending the mail to the correct person/s.

See the Trust's E-mail Policy for more detailed information.

3. Home working

Confidential information should not be removed from site for home-working purposes.

PLEASE RETAIN THE CODE OF CONDUCT FOR YOUR INFORMATION