Tower Hamlets GP Care Group
Receipt and Transfer of Information Policy

Date Issued	23rd February 2017
Date to be reviewed	Periodically or if statutory changes are required
Title	Receipt and Transfer of Information
Supersedes	All previous Policies
This policy will impact on	All staff
Financial Implications	No change
Policy Area	Information Governance
Version No	2.0
Issued By	Chris Banks
Author	Ruth Walters
Document Reference	
Effective Date	01/04/2017
Review Date	01/04/2019

1.1.1 Approval Record

	Committees / Groups / Individual	Date
Consultation	Governance Committee	
Approved by	Dr Joe Hall Chair, Governance Committee	2/5/17

Receipt and Transfer of Information Policy

1-Introduction

THGPCG provides healthcare to patients in a variety of settings and services to fulfill its core purpose. Processing information is a fundamental, routine part of the healthcare process and includes personal identifiable information in both electronic and paper records for both staff and patients.

On occasions telecommunications are used to transfer information containing personal identifying information, both to and from external locations.

2- Equality & Diversity

THGPCG is committed to an environment that promotes equality and diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy should be implemented with due regard to this commitment

3 Objectives

It is well documented that the use of telecommunications without appropriate controls is an insecure method of transferring confidential information. However, currently, there are limited alternatives to this transfer method. The objectives of this policy are: -

- To raise staff awareness of the risks associated with the use of manual and electronic systems when transferring confidential information
- To encourage the limiting and/or anonymisation/pseudoanonymisation of confidential patient information wherever possible in regard to all methods of transporting information.
- To ensure that all fax machines are used appropriately in accordance with location and guidelines laid down in this policy
- To ensure that the email system is used appropriately and in accordance with the guidelines laid down in this policy
- To ensure that the correct procedures for the transportation and posting of information are adhered to
- To make staff aware of the correct procedures regarding telephone conversations
- To make staff aware of the procedures around automated electronic communications out of the THGPCG e.g. hospitals

4-Scope of Policy

2 This document offers guidance to all staff transmitting or receiving confidential patient or staff information via telecommunications either to or from internal and external locations. This policy also includes any paper/manual records that are transported between THGPCG sites. This includes the use of telephone, postal services, email, internet, fax and physical movement of confidential and sensitive records. This list is not exhaustive.

5- Policy

5.1 Contacting Patients by Telephone

When contacting patients by telephone, the following guidelines should be followed:

- Ring the number in the health record unless alternative arrangements have been made with the patient/staff member
- Always ask for the patient by full name to ensure that you are speaking to the correct person and seek verification through confirmation of details, such as date of birth etc.
- Do not leave messages with another person without prior agreement
- Do not leave messages on answer machines if there is any doubt of who the call is meant for unless the call is urgent, and then a name and contact number should be left. The name of the service should not be left
- Ensure that the patient is able to discuss the purpose for the phone call and if this is not possible, arrange to call back at another time
- Ensure that at all time confidential information is not disclosed to any person other than the patient, unless prior consent has been obtained and recorded. If challenged over refusal to give out patient information, refer the matter to a supervisor.
- Be aware of the dangers of leaving messages – have you got the correct number; who might hear the message; will the recipient understand the message and how can you be certain that the patient has received the message
- Where telephones are to be recorded (for example in the OOH service) service users must be made aware of the recording before the exchange of any sensitive information is undertaken.

5.2 Contacting Patients by automated telephone or text message

Automated telephone messaging and text messaging can be used to contact patients to remind them of future appointments, or to advise patients to contact the department. Consent is assumed from the patients through fair processing notices in the form of posters, letters and leaflets. The following must be adhered to when using this form of communication:

- The patients record is checked for their contact number
- Automated systems would contact the patient with regard to forthcoming appointments and the system would endeavor to physically contact the patient on their landline, or by text message to a mobile telephone
- The text message should not contain any information that would breach patient confidentiality if seen by someone else
- The patient has a choice to opt out of the system and once a request is received from the patient, a confirmation letter should be sent to the patient

5.3 Contacting Patients by email

Many patients contact clinicians by email asking a variety of questions including requests for clinical information. When responding to patients by email, the following guidelines must be adhered to:

- The patient will probably have contacted the clinician using a generic non secure email such as hot mail account. Personal, sensitive information must not be sent from NHS net and/or Barts Health to these accounts. If the patient has requested other, non-sensitive information such as appointment details, a response can be made to these accounts
- If the patient requests personal, sensitive information you should not respond to the request but rather suggest a face-to-face or telephone conversation. This should be in the form of a new re-mail and not as a response to the original request as this would further risk confidentiality

5.4 Contacting Healthcare Professionals

When contacting other healthcare professionals the following guidelines should be adhered to:

- If the conversation is by telephone, ensure that where possible, the conversation cannot be overheard by any person not directly involved with the persons care.
- Use a published or internal directory to identify a telephone number to contact the individual
- Ask for the member of staff by name and if not available call back at a later time or request a return call. Personal information should not be divulged as part of the message.
- If using e-mail to communicate, ensure that emails are sent between the same secure system. If using NHS net then only NHS net addresses may be used (these end in @nhs.net). Ensure that the correct email address is used (your email default address book should be set to 'all users' not 'global' to ensure accidental selection of an e-mail address is avoided). If email to a Barts Health address is required (for example when communication with a ward is required) then the email must be generated from a Barts Health address.

5.5 Communication relating to Staff Members

When a telephone call is received relating to a staff member, the following guidelines should be adhered to:

- Information should not be given out over the telephone about a staff member. Home address and telephone numbers should never be divulged without consent
- In the event of an urgent query, take details from the caller and contact the member of staff so that they can respond
- If the member of staff is not on duty, the line manager should be informed who will then take any appropriate steps in relation to contacting the member of staff
- Any companies requesting confirmation of an employee's position, salary etc. should be asked to make the request in writing to the Information Manager
- If using e-mail to communicate, ensure that only NHS net addresses are used (these end in @nhs.net). Ensure that the correct email address is used (your email default address book should be set to 'all users' not 'global' to ensure accidental selection of an e-mail address is avoided).

5.6 Automated electronic communication outside of the THGPCG

Under no circumstances should person identifiable data be sent to any other organisations without using NHS net accounts. Electronic information such as discharge summaries are sent using encrypted data transfer services which are both secure and reliable. The use of fax machines for sensitive data should only be used when it is absolutely necessary for the provision of care. Before sending the fax staff must check with the intended recipient that incoming faxes are accessible only to authorised staff (this may be done in advance for organisations with whom the service has regular communications). Pre-programmed numbers should be used wherever possible to avoid mis-dialing. A cover sheet should be sent containing a confidentiality statement. Only the minimum amount of information should be sent to ensure care delivery.

5.7 Mail service for transferring data via external mail

When sending information outside of the THGPCG using the normal postal system, the following guidelines should be adhered to:

- Confirm the name, department and address of the recipient. Incorrectly addressed mail could result a breach of the Data Protection Act and/or delayed delivery
- Seal the information in a robust envelope
- Mark the envelope "Private & Confidential to be opened by addressee only"
- Enter a return address on the back of the envelope
- Dependent on the information a signature may be required to provide proof of delivery or receipt
- Where appropriate, send the information by recorded delivery
- Request a confirmation of receipt from the recipient

- When sending information via post where the recipient might not be clear as to the identity of the sender, staff should ensure that either a compliment slip is included or that the enclose clearly states the name, title and contact details of the sender

5.8 Mail service for transporting personal identifiable data via internal mail

When sending patient identifiable information internally, the following guidelines should be adhered to:

- The internal address of the intended recipient should be confirmed
- The envelope should be sealed and addressed to the full location of the recipient
- Incoming mail is to be opened away from public areas and by the addressee or designated personnel only
- Confirmation of receipt may be sought to ensure delivery has occurred
- When sending information via post where the recipient might not be clear as to the identity of the sender, staff should ensure that either a compliment slip is included or that the enclose clearly states the name, title and contact details of the sender

5.9 Secure Data Transportation

Manual person identifiable information (other than health records) must not be removed from THGPCG premises without assessment. If it is absolutely necessary to transport manual lists etc. to support patient care then data flow mapping and risk assessment must be completed first. The assessment must justify the continued transportation of manual information (rather than electronically held encrypted information) and be logged with the Information Manager. All removable media (laptops, USB sticks, PDAs etc.) must be encrypted and secure. All flows of electronic personal identifiable information must be mapped and logged with the THGPCG Information Manager. All personal identifiable data flows such as external email, fax etc. must be mapped and risk assessed. All flows must be reviewed annually. Data flows identified as medium or high risk must have a solution to reduce the risk. (Refer to appendix A and B for templates)

When health records are taken off site the following guidance must be adhered to:

- Record what information you are taking off site and why, and if applicable, where and to whom you are taking it
- Provide a contact telephone number, so contact can be made in case information is required urgently back on site
- Information must be in a sealed container
- Information must be transported via a THGPCG approved courier or by the health professional themselves
- It must be transported directly from site to site without any unauthorized stops
- Patient identifiable information must never be left unattended at any time
- Information must be returned to the site as soon as possible, and by day end
- Record that the information has been returned

5.10 THGPCG Facsimile locations

All locations must be risk assessed for risks to confidentiality. This will identify the risks attached to each location and assign one of the following two categories:

1. A secure fax location
2. A non-secure fax location

Only designated secure fax machines should be used for the transmission and/or receipt of confidential staff or patient information

Fax Location Criteria:

- **Level 0** Access to fax location available to general public/patients therefore the location is not secure
- **Level 1** Access to fax location is by staff only and therefore the location is secure
- **Level 2** Access to fax location is by designated staff only and therefore the location is secure

If the fax machine is to be left switched on outside of office hour's arrangements must be in place to ensure that all staff (e.g. cleaning staff) have signed a confidentiality clause to prevent unauthorized access to incoming documents.

5.11 THGPCG Facsimile Ownership

There must be a clearly defined delegated 'local' ownership and responsibility at an operational level for faxed information. Where practical named individuals shall be identified as designated staff, managing the fax transfers of confidential information on a day to day basis. However where local requirements dictate that all staff need to access fax use, then senior staff will nominate an individual who will ensure that all staff are aware of their own responsibilities, and will monitor activity to ensure appropriate use.

5.12 Regular (unavoidable) internal/external transfer of confidential patient information

In these circumstance senior staff members from each location i.e. sender and recipient, must liaise to agree the following

- The inclusion of patient identifiable data items is both necessary and justified for the purpose of the flow of information
- Both locations have a list of designated staff names at the other location
- In areas with high volume faxing or large staff groups both areas should have a designated individual who will ensure that all users are aware of their responsibilities and will monitor activity to ensure that all the requirements of this policy are met
- Both fax locations are secure and local arrangements are made regarding transfers i.e. at a specific time, with a confirming phone call or a double fax etc.

5.13 Circumstances when a fax should not be used

Sensitive patient information

Information such as that concerning HIV status; venereal disease; drug misuse; incriminating evidence (this list is not exhaustive) should **never** be transmitted via fax.

5.14 Transcribing of Telephone Message

Recorded telephone message containing person identifiable information or sensitive information such as names and addresses of application telephoning for a job application must be received into a secure location, so that only those entitled to listen to the message my do so whilst it is played back.

If a message book is used to note message for absent staff, this should also be stored in a secure location

5.15 Pigeon-holes/In Trays for Paper Information

Regular housekeeping must be carried out in areas where pigeon-holes or pin-trays are used to disseminate corporate and person/patient identifiable information. Nothing should be left in these overnight. In addition, any visit, appointment or message book must be stored in a secure area when not in use.

5.16 Incident Reporting

THGPCG records incidents relating to information security as minor, significant or major in line with the corporate risk register.

A security incident is defined as any event, which has resulted, or could have resulted in:

- The disclosure of any confidential information to any unauthorized individual
- The availability of the system or information being put at risk
- An adverse impact, for example embarrassment to the organization/NHS, threat to personal safety or privacy, legal obligation or penalty, financial loss, disruption of activities

The majority of security breaches are innocent and unintentional, for example a misdialed number which was noticed before transmission (this would be a minor occurrence), but

the transmission of patient information to the wrong recipient due to misdialed number would be more serious in nature

Loss of personal identifiable information may result in the initiation of the Serious Untoward Incident Process. Staff is responsible for reporting any actual or suspected breaches of security or potential weakness in secure operations of any systems.

6.0 Roles and Responsibilities

This policy is the responsibility of the Chair of the Information Governance Committee

6.1 Managers

The Chief Executive (via heads of service and all staff) is responsible for ensuring the confidentiality of patient information. THGPCG must comply with current data protection legislation and the recommendations of the Caldicott report to maintain the confidentiality of patient information by limiting access.

The following forms the basis of a compliance framework:

1. The Head of Service or nominated representative is responsible for identifying all staff. A log of names, signatures and responsibilities including fax access should be retained locally. Arrangements must be made to record staff changes
2. The Head of Service or nominated representative is responsible for the annual mapping and risk assessment of all person identifiable data flows. Management is also responsible for ensuring that all portable and removable media is encrypted to NHS standards.
3. The Head of Service is locally responsible for the provision of staff training. All staff must be fully aware of the guidance provided in this policy, it's requirements and implementation

6.2 Staff

Staff must be aware of the guidelines around the use of all methods of communication contained in this policy and adhere to the procedures.

7.0 Associated Documentation and References

This policy should be read in conjunction with

- THGPCG Code of Conduct Policy
- THGPCG Information Security Policy
- THGPCG Records Management Policy
- THGPCG Information Governance Policy
- THGPCG Mobile and Teleworking Policy

Training & Resources

The implementation of policies in this area will be carried out by all THGPCG staff and will be led by the Information Governance Committee and designated management staff. Training will be dictated by staff roles and all staff, as a minimum, are required to undertake Bluestream Information Governance training annually.

6-Monitoring & Audit

The information governance toolkit will be used to conduct a baseline audit and construct action plans for future compliance with this agenda.

THGPCG will maintain a corporate risk register and is the responsibility of all staff within the organization to inform the risk agenda

Appendix A
Risk Assessment

A risk assessment will be undertaken for each fax machine that is used to send or receive patient identifiable information.

That risk assessment will cover: -

- Location of the machine,
- Access to the machine,
- Procedures covering the receipt of patient identifiable information,
- Procedures covering the dispatch of patient identifiable information,
- Housekeeping standards (e.g. stored fax numbers, fault reporting, and consumables).

It will be undertaken in 3 steps, using the attached documentation:-

Step 1 "Risk Assessment checklist" – used to identify the potential for a breach in confidentiality.

Step 2 "Risk Assessment" – undertaken when stage 1 has identified the potential for a breach. This will produce a "risk score" by assessing the "consequence and possibility" of each risk.

Step 3 "Detailed Risk Assessment" – undertaken when a risk scores above 4. This will identify the measures that will be put in place to manage the risk.

Step 4 Risk action plan – Summary of risk, action to be taken and target time. Copies of above should be sent to Ruth Walters, Interim Director of Quality & Assurance.

STEP 1 - FAX RISK ASSESSMENT CHECKLIST

Area to be assessed:_____ **Fax Number**_____

Patient Identifiable Information Confidentiality Risks	Delete if not applicable	
1 Risk of public accessing information		
1.1 Is the fax machine located in a public area?	YES	NO
1.2 Is the fax machine visible from a public area?	YES	NO
1.3 Is the fax machine left unattended at any time?	YES	NO
1.4 Are incoming faxes left on or around the fax machine?	YES	NO
1.5 Are sent faxes left on or around the fax machine?	YES	NO
2 Risk of fax being sent to the wrong recipient		
2.1 Does the fax machine have a memory for storing recipients fax numbers?	YES	NO
2.2 Are recipients fax numbers entered each time a fax is sent?	YES	NO
2.3 Are fax numbers always checked with recipients to ensure they are correct?	NO	YES
3 Risk of fax not being received		
3.1 Does the fax machine have a paper supply?	YES	NO
3.2 Does the fax machine require printing consumables (ink drum, toner)?	YES	NO
3.3 Is the fax machine power supply turned off at any time?	YES	NO
3.4 Does the fax machine have a tray to collect received faxes?	NO	YES
4 Risk of other staff accessing information		
4.1 Do other non-directorate / dep't staffs have access to the fax machine?	YES	NO
4.2 Is the fax machine kept in a locked room when unattended?	NO	YES

If shaded column has any responses not deleted, then Step 2 risk assessment form needs to be completed.

STEP 1 – EXTERNAL E-MAIL RISK ASSESSMENT CHECKLIST

NB This applies to organization sensitive data only, patient identifiable information must not be sent to external e-mail addresses

Area to be assessed:_____

Patient Identifiable Information Confidentiality Risks	**Delete if not applicable**	
1 Risk of public accessing information		
1.1 Is the computer screen visible to members of the public?	Yes	No
2 Risk of Email being sent to the wrong recipient		
2.1 Are email addresses always checked with recipients to ensure they are correct?	NO	YES
2.2 Has a contact card been created for the intended recipient?	NO	YES
3 Risk of email not being received		
3.1 Is the 'junk' email box checked daily?	NO	YES
3.2 Is the read receipt request enabled?	YES	NO
4 Risk of other staff accessing information		
4.1 Is the computer screen visible to other members of the workforce and/or members of the public?	YES	NO
4.2 Is the computer screen locked when the station is unattended?	NO	YES

If shaded column has any responses not deleted, then Step 2 risk assessment form needs to be completed.

Assessment Number:_____ **STEP 2 - RISK ASSESSMENT**

Department:_____ **Location:**_____

Assessor:_____

Date:_____ **Page Number:**_____ **Manager:** _____

RISKS IDENTIFIED:	CONTROL MEASURES ALREADY IN PLACE		Likelihood 1 - rare 2= unlikely 3 - possible 4 - likely 5 - certain	Consequence 1 = Insignificant 2 = Minor 3 = Moderate 4 = Major 5 = Catastrophic	Risk Rating Grading of Very Low, Low Moderate or High	Further Assess-ment Required Y/N (YES PROVIDED RISK RATING NOT VERY LOW OR CONSEQUENCE WAS NOT INSIGNIFICANT)

STEP 3 - DETAILED RISK ASSESSMENT

Department/Location:_____ **Date:**_____ **Assessor:**

_____

Risk Assessed: _____

RISK		Consequence	Probability	Risk Rating
1				
2				
3				
4				
5				
	RISK POTENTIAL SCORE			
FACTORS WHICH INCREASE RISK				
1				
2				
3				
4				
CONTROLS NEEDED TO REDUCE POTENTIAL ***(in order of priority)***				
1				
2				
3				
4				
	REVISED SCORE IF CONTROLS PUT IN PLACE			
OTHER MEASURES RECOMMENDED				
1				
2				
3				
4				
REVIEW DATE:		MANAGER:		

Risk Assessment
Date of this assessment
Date of last assessment

ACTION PLAN

No	Action Required	Priority	Action By	Target Date	Completion Date

Department/Directorate _____ Location _____

Assessor _____ Designation _____

Incident Severity Table

0	No significant reflection on any individual or body Media interest very unlikely. Minor breach of confidentiality. Only a single individual affected.	No need to record in annual report
1	Damage to an individual's reputation. Possible media interest e.g. celebrity involved. Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted.	Annual Report
2	Damage to team's reputation. Some local media interest that may not go public. Serious potential breach and risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected.	Annual Report
3	Damage to a services reputation/ Low key local media coverage. Serious breach of confidentiality e.g. up to 100 people affected.	SHA Information Commissioner
4	Damage to an organisations reputation/ local media coverage. Serious breach with either particular sensitivity E.g. sexual health details or up to 1000 people affected.	SHA Information Commissioner
5	Damage to NHS reputation/ National media coverage. Serious breach with potential for ID theft or over 1000 people affected.	SHA Information Commissioner