Trust-wide Document

Great Western Hospitals NHS Foundation Trust

Clinical Systems Access Monitoring and Audit Policy

Document No	IG - 00002	**Version No**	2.0
Approved by	Policy Governance Group	**Date Approved**	13/11/19
Ratified by	Information Governance Steering Group	**Date Ratified**	01/11/19
Date implemented (made live for use)	14/11/19	**Next Review Date**	01/11/22
Status	LIVE		

Target Audience- who does the document apply to and who should be using it. - The target audience has the responsibility to ensure their compliance with this document by: • Ensuring any training required is attended and kept up to date. • Ensuring any competencies required are maintained. • Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.	All users who are authorised to access the Trust's clinical systems and the NHS Summary Care Record. This group comprises mainly employees employed by or contracted to the Trust, including bank, agency and volunteers, but also includes certain staff employed by other organisations, including those external to the NHS.
Special Cases	None
Accountable Director	Director of Finance / SIRO
Author/originator – Any Comments on this document should be addressed to the author	Senior Information Governance Officer
Division and Department	Corporate / Finance
Implementation Lead	Head of Information Governance / Data Protection Officer
If developed in partnership with another agency ratification details of the relevant agency	N/A
Regulatory Position	• Data Protection Act 2018 (Ref 12) • Computer Misuse Act 1990 (Ref 13) • Caldicott Principles (Ref 1)
Review period. This document will be fully reviewed every three years in accordance with the Trust's agreed process for reviewing Trust -wide documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.	

Contents

1 Introduction & Purpose

1.1 Introduction & Purpose

In compliance with legal and professional standards (see Section 5.2), Great Western Hospitals NHS Foundation Trust (the Trust) is committed to ensuring the highest level of patient confidentiality. Access to the Trust's clinical Information Technology (IT) systems, although restricted by a level of role-based access rights in line with Caldicott Principles (Ref. 1) and the Trust's Data Security and Protection Policy (Ref. 2), are not immune to breaches of patient confidentiality by authorised users (hereby defined as any person authorised to use a particular IT system).

The National Health Service (NHS) Care Record Guarantee (Ref. 3) requires that all NHS organisations put in place mechanisms to ensure that confidential information is protected. This requires access to confidential information to be monitored and audited locally and, in particular, requires that there are agreed procedures for investigating confidentiality alerts.

It is also a requirement of the Data Security and Protection Toolkit [DSPT] (Ref. 4) that the Trust establishes appropriate confidentiality audit procedures to monitor access to confidential patient information. Therefore, the Trust has introduced a proactive programme of clinical system audits, acting as both a deterrent and a means of identifying potential violations to patient confidentiality through inappropriate use of clinical systems, such as the Medway patient administration system/electronic patient record (PAS/EPR) system.

The purpose of this document is to define the Trust's approach to auditing access to patient information on the Trust's clinical systems, including Medway PAS/EPR and the NHS Summary Care Record (see Section 2.5) and the monitoring of potential inappropriate use of the systems.

1.2 Glossary/Definitions

The following terms and acronyms are used within the document:

DHSC	Department of Health & Social Care
ED	Emergency Department
EPR	Electronic Patient Record
GP	General Practitioner
IG	Information Governance
IGSG	Information Governance Steering Group
IR1	Incident reporting system
IT	Information Technology
Medway	The proprietary name of the Trust's PAS/EPR system
NHS	National Health Service
PALS	Patient Advice & Liaison Service
PAS	Patient Administration System
SCR	Summary Care Record
User	Any person authorised to use an IT system

2 Main Document Requirements

2.1 Audit Scope

The Medway PAS/EPR system constitutes the current core hospital system holding patient data. However, the approach detailed in this document may be applied, for the purpose of ensuring patient confidentiality, to other clinical IT systems which provide adequately detailed audit trails.

2.2 Audit Aim & Objectives (Clinical Systems)

Aim

- To manage the risks surrounding inappropriate access to patient information through the use of clinical systems.

Objectives

- To ensure that authorised users of clinical systems access patient information only in compliance with patient confidentiality legislation, such as the Data Protection Act 2018 and national and Trust policies, such as the Caldicott Principles (Ref.1) and the Data Security and Protection Policy (Ref. 2).
- To inform the escalation of suspected breaches of patient confidentiality via the Trust's Data Security & Protection Incident Reporting Procedure (Ref. 9) and IR1 incident reporting system, and, if necessary, through the disciplinary process.
- To act as a deterrent to users who may be tempted to breach patient confidentiality.

2.3 Reactive Audits

Audit reports can be produced either at user-level to identify patient records that have been accessed by a specified user, or at patient-level to identify users who have accessed patient record(s).

2.3.1 User Level Audits

If any user of the Trust's clinical information technology (IT) systems is suspected, by any other user or employee, of inappropriate use of the systems, or of non-compliance with legislation and standards surrounding patient confidentiality, the incident should be reported in the first instance in accordance with the Data Security & Protection Incident Reporting Procedure (Ref. 9). The Trust may also monitor and audit the use of clinical systems as part of a complaint from a service user.

A user-level audit may be requested as part of an investigation process at any time, normally by the line manager or other senior manager. The IG Team or the IAA of the system will provide the audit report if it is appropriate to do so in compliance with national and local legislation and Trust policies, such as the Information Governance Policy (Ref. 7) and the Data Protection Policy (Ref. 10).

2.3.2 Patient-Level Audits

If it is suspected that the confidentiality of the records held in a clinical system for any patient or group of patients may have been put at risk, a patient-level audit may be requested through the IG Team. Requests may also be received from the Patient Advice and Liaison Service (PALS) following a complaint from the patient or their representative about a suspected breach of confidentiality. The IG Team will provide the audit report if it is appropriate to do so in compliance with national and local legislation and Trust policies, as per section 2.3.1.

2.4 Proactive Programme of Audits

In addition to reactive audits, the IG Team runs a monthly programme of proactive audits. On a rolling three-monthly cycle, a random selection of internal users, patients and external users (normally those from partner organisations) are audited.

2.4.1 User Selection Criteria

A report is generated from the Medway PAS system showing a completely random selection of user names to be audited. All users at all levels across the Trust that access the clinical systems are included in the selection criteria.

User-level audit reports are generated on a rolling three-monthly basis for a percentage of the user base, that the IG Team use for further investigation and validation as described in the "Audit Review" section 2.5 below. The IG Team will forward any concerns to the relevant manager(s) responsible for authorising the user's access to the clinical system.

In the event that a member of the IG team appears on the randomised user-level list to be audited, the responsibility to complete this will fall to the Information Asset Owner, delegated to the Information Asset Administrator. This separation will maintain the independence of the audit and ensure any potential concerns can be escalated to the user's line manager, the system IAO or the Caldicott Guardian as required.

2.4.2 Patient Selection Criteria

A list of random patient hospital numbers for which the proactive patient level audits will be undertaken is selected using reports generated from the Medway system for in-patients, outpatients and patients attending the Emergency Department (ED). The patients chosen at random will have had appointments with the Trust in the previous month from that in which the audit is undertaken.

Patient-level audit reports are generated on a rolling three-monthly basis, interspersed with user-level audits for Trust employees and for non-Trust users. Results will be scrutinised by the IG Team for investigation in the first instance.

2.4.3 General Practitioner (GP) User Audits

GP users are included in the proactive user-level audits, but additional user-level audits may be run on a practice-by-practice basis. Access requirements are checked for any GP who has not logged on to the clinical system, usually Medway, for more than six months, and accounts may be disabled where appropriate.

2.4.4 Non-Trust Audits

On a three-monthly basis, interspersed with general user-level and patient-level audits, user-level audits are carried out which concentrate on users who are not employed by the Trust, but work for other partner organisations that have been granted access to clinical systems.

2.5 Audit Review

Audit results will be analysed by the IG Team in the first instance. The job role of the user, at the time of access to the patient record, will be matched against the care activity necessary for the access made as shown in the audit report.

The IG Team will monitor repeated access to patient information, successful access of patient information by potentially unauthorised persons and will highlight any potential evidence of shared login sessions/passwords – for example:

- Evidence of potential unauthorised access might be a nurse on Dove Ward accessing patients on Saturn Ward, or a midwife accessing records of adult male patients;
- Evidence of shared logins/passwords might be some activity that carries over 12 hours, i.e. longer than a shift pattern.

Queries and potential areas of concern will be highlighted to the Authorising Manager (the manager responsible for authorising the user's access to the clinical system). The Authorising Manager will be required either to confirm that the user had a lawful and appropriate requirement to access the patient(s) record(s), or to request further action, e.g. an investigation, in accordance with the Trust's Data Security & Protection Incident Reporting Procedure (Ref. 9). The forms used for this process are shown at Appendices D – Clinical System Access Level Validation Form, and E – Audit Validation Form.

As part of the audit review, the Authorising Manager will be asked to confirm the group-level access of the audited employee. Where access is deemed inappropriate, the IT Department's Clinical Applications Team will amend the user's access as appropriate, within the limitations of the clinical system, and as authorised by the user's current Authorising Manager.

2.6 Summary Care Record (SCR) Audit

The IG Team act as the Trust's Privacy Officers in respect of the NHS Summary Care Record (SCR). The SCR system is accessed by employees working in the Pharmacy and in the Urgent Care Centre at the Great Western Hospital (referred to as SCR users), in order to check current medication for in-patients. When an access is made, the user is expected to have a legitimate relationship with the patient and to have asked the patient to confirm their consent to access the record – this is known as a 'self-claim' alert. If the patient is unable to consent, for example they may have dementia or be unconscious or be extremely unwell, the SCR user can still access the record but must use the "SCR Access made in an emergency alert". In this case the SCR user must also complete a free text field which explains why this type of access was used e.g. patient unresponsive or patient has dementia.

The Privacy Officer will review each alert to check that the patient concerned was under the care of the Trust at the time the alert was raised. The Privacy Officer will also check that explanations given for the access to a patient's record are reasonable.

The NHS Spine is used to produce a report of the alerts generated within the last week to compare with the weekly in-patient report (for Pharmacy staff) and the monthly ED report (for Urgent Care Centre staff), which is provided by the Trust's Information Team. A spreadsheet that compares the results of both reports is used to do this. Most alerts will show up as "NHS number on PAS extract" and the spreadsheet cell will turn green.

If the NHS number for the alert does not match the in-patient report, the cell will turn red and state "Not in PAS Extract or No NHS Number Available". In this case the Privacy Officer will look up the patient's full details on the NHS spine record and will check this against the relevant patient record in the Medway PAS/EPR system. In most cases, this will be a legitimate access, but the NHS number may not have been completed, or a duplicate patient record may have been created.

If the Privacy Officer cannot match the record, or has concerns about the reasons for using an emergency alert, they will contact the Pharmacy manager or the Urgent Care Centre manager in the first instance. If the reason for access cannot be justified, or there are concerns then the disciplinary process as described below in Section 2.7 will be followed.

Should SCR access be rolled-out to other Trust employees, the Privacy Officers will continue to monitor the alerts generated as described above, but will use additional reports provided by the Information Team, for example for outpatients or patients attending the Emergency Department.

2.7 Disciplinary Process

Areas for concern, identified as an outcome of the audit review by the IG Team and validated as a potential issue by Authorising Managers will be investigated in accordance with the Trust's Data Security & Protection Incident Reporting Procedure (Ref. 9) and the employee(s) concerned may be subject to disciplinary proceeding in line with the Trust's Conduct Management Policy (Ref. 11).

Where a partner organisation requests and is permitted access to a clinical system for their employee(s), any potential breach of patient confidentiality identified as a result of an audit review will be notified to senior members of the organisation's employees, the Human Resources team or the IG Team within the partner organisation, as appropriate. It is expected that disciplinary processes within the relevant organisations will be invoked. The IG Team will ensure follow-up, escalating the issue to the Trust's IG Steering Group, Caldicott Guardian, SIRO and, if appropriate, enlisting the assistance of outside organisations to undertake further investigations.

For incidents of a serious nature which may result in disciplinary action and/or criminal prosecution, the investigation may be handled by senior Trust managers and/or outside organisations that have the relevant experience and expertise to conduct such an investigation.

2.8 Reporting

Any potential breach of patient confidentiality or security will be reported to the IG Steering Group on a monthly basis by the IG Team. Serious incidents will be reported on the Data Security and Protection Toolkit (DSPT) and notified to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Statistics relating to the audits e.g. numbers of audits performed, number of inconsistencies found etc. will be reported on an annual basis to the IG Steering Group.

3 Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below: -

Measurable policy objectives	Monitoring or audit method	Monitoring responsibility (individual, group or committee)	Frequency of monitoring	Reporting arrangements (committee or group the monitoring results is presented to)	What action will be taken if gaps are identified
Monthly audits have been completed in accordance with this policy (100%)	Report to relevant committee on audit of usage as detailed in Section 2.1	IG Team	Annually	IG Steering Group	An action plan will be developed to address any issues which will be

Trust's Disciplinary process has been followed	Report to relevant committee	IG Team	As required	IG Steering Group	monitored by the IG Steering Group / PRC.

4 Duties and Responsibilities of Individuals and Groups

4.1 Chief Executive

The Chief Executive is ultimately responsible for the implementation of this document.

4.2 Ward Managers, Matrons and Managers for Non Clinical Services

All Ward Managers, Matrons and Managers for Non Clinical Services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

4.3 Caldicott Guardian

The Caldicott Guardian has overall responsibility for ensuring that access to confidential patient information is monitored and audited and for ensuring that confidentiality audit procedures are developed and communicated to all employees. This responsibility may be delegated to the IG Team.

4.4 Clinical System Users

All clinical system users must ensure that they are aware of their responsibilities regarding patient confidentiality and must adhere to legislation, national and local standards. Details of this can be found in the documentation, listed in Regulatory Position, which is located on the Trust's Intranet and the Department of Health & Social Care website. Every user of clinical information systems is required to sign a confidentiality form before being given the appropriate access to the system(s) needed for their role and responsibilities. The terms and conditions stated on the form are shown at Appendix C - . Confidentiality Conditions for Clinical System Users.

4.5 Authorising Managers

All managers who authorise access for their employee(s) to the Trust's clinical IT systems must report any suspected breaches of patient confidentiality to the IG Team or via the Trust's incident reporting (IR1) system and, if necessary, assist the IG Team to review the audit reports produced. If necessary the manager must invoke the disciplinary process as described in the Trust's Conduct Management Policy (Ref. 5).

Authorising Managers will be expected to validate user access in line with job requirements using audit validation forms at Appendix D – Clinical System Access Level Validation Form, and Appendix E – Audit Validation Form, where necessary, as per Section 4 of this policy.

4.6 Clinical Applications Team

The Clinical Applications team will affect any authorised changes to user group access, in line with role-based access and within the clinical system(s) limitations.

4.7 Request Fulfilment Team

The Request Fulfilment Team is responsible for setting up and disabling user accounts to the systems, in line with requests from line management and medical staffing (for Locums).

4.8 Information Governance Team

The IG Team will undertake the audit reviews as detailed in "Audit Review" section and highlight any potential threat to patient confidentiality identified through the audit review, using the forms at Appendix D – Clinical System Access Level Validation Form, and Appendix E – Audit Validation Form. They will collate satisfactory responses, i.e. responses where Authorising Managers can confirm the audited user has accessed patient records only in the course of the patient's care and had a justifiable need to do so.

The IG Team will investigate, in accordance with the Trust's Data Security & Protection Incident Reporting Procedure (Ref 9), any potential breaches to patient confidentiality, e.g. instances of highlighted user access that cannot be validated or approved by the relevant Authorising Manager and escalate identified issues in accordance with the above procedure.

The IG Team undertake the role of Privacy Officers for the Trust and they have additional responsibilities for overseeing privacy and security in the Trust and for monitoring access to the NHS Summary Care Record – see Section 2.5.

4.9 Human Resources Department

The Human Resources Department is responsible for any investigations in accordance with the Trust's Conduct Management Policy (Ref. 11) in conjunction with Trust managers as deemed appropriate to the severity of the incident.

4.10 Document Author and Document Implementation Lead

The document Author and the document Implementation Lead are responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

4.11 The Information Governance Steering Group

The IGSG will receive reports of any inappropriate access discovered as a result of monitoring access and will receive reports of the number of audits undertaken and the results on an annual basis.

5 Further Reading, Consultation and Glossary

5.1 References, Further Reading and Links to Other Policies

The following is a list of other policies, procedural documents or guidance documents (internal or external) which employees should refer to for further details:

Ref. No.	Document Title	Document Location
1	Caldicott Principles	T:\Trust-wide Documents
2	Data Security & Protection Policy	T:\Trust-wide Documents
3	NHS Care Record Guarantee	systems.hscic.gov.uk

Ref. No.	Document Title	Document Location
4	Data Security & Protection Toolkit	https://www.dsptoolkit.nhs.uk/
5	Confidentiality: NHS Code of Practice	www.gov.uk
6	Information Security Management – NHS Code of Practice – 2007	www.gov.uk
7	Information Governance Policy	T:\Trust-wide Documents
8	IT Equipment Usage Policy	T:\Trust-wide Documents
9	Data Security & Protection Incident Reporting Procedure	T:\Trust-wide Documents
10	Data Protection Policy	T:\Trust-wide Documents
11	Conduct Management Policy	T:\Trust-wide Documents
12	Data Protection Act 2018	http://www.legislation.gov.uk
13	Computer Misuse Act 1990	http://www.legislation.gov.uk

5.2 Consultation Process

The following is a list of consultees in formulating this document and the date that they approved the document:

Job Title / Department	Date Consultee Agreed Document Contents
Clinical Risk Advisor	11 October 2019
Deputy Health Records Manager	14 October 2019
Head of IT Applications & Projects	18 October 2019
Head of HR & Wellbeing Services	24 October 2019
Clinical Application Manager	24 October 2019

6 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been completed for this document and can be found at Appendix A.

Appendix A - STAGE 1: Initial Screening For Equality Impact Assessment

At this stage, the following questions need to be considered:			
1	What is the name of the policy, strategy or project? **Clinical Systems Access Monitoring and Audit Policy**		
2.	Briefly describe the aim of the policy, strategy, and project. What needs or duty is it designed to meet? Policy details the proactive and reactive programme of clinical system audits, acting as both a deterrent and a means of identifying potential violations to patient confidentiality		
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any of the nine protected characteristics (as per Appendix A)?		**No**
4.	Is there evidence or other reason to believe that anyone with one or more of the nine protected characteristics have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?		**No**
5.	Has prior consultation taken place with organisations or groups of persons with one or more of the nine protected characteristics of which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?		**No**

Signed by the manager undertaking the assessment	Mark Arnold
Date completed	8th October 2019
Job Title	Head of IG and DPO

On completion of Stage 1 required if you have answered YES to one or more of questions 3, 4 and 5 above you need to complete a STAGE 2 - Full Equality Impact Assessment

Equality Impact Assessment

Are we Treating Everyone Equally?

Define the document. What is the document about? What outcomes are expected?

Consider if your document/proposal affects any persons (Patients, Employees, Carers, Visitors, Volunteers and Members) with protected characteristics? Back up your considerations by local or national data, service information, audits, complaints and compliments, Friends & Family Test results, Staff Survey, etc.

If an adverse impact is identified what can be done to change this? Are there any barriers? Focus on outcomes and improvements. Plan and create actions that will mitigate against any identified inequalities.

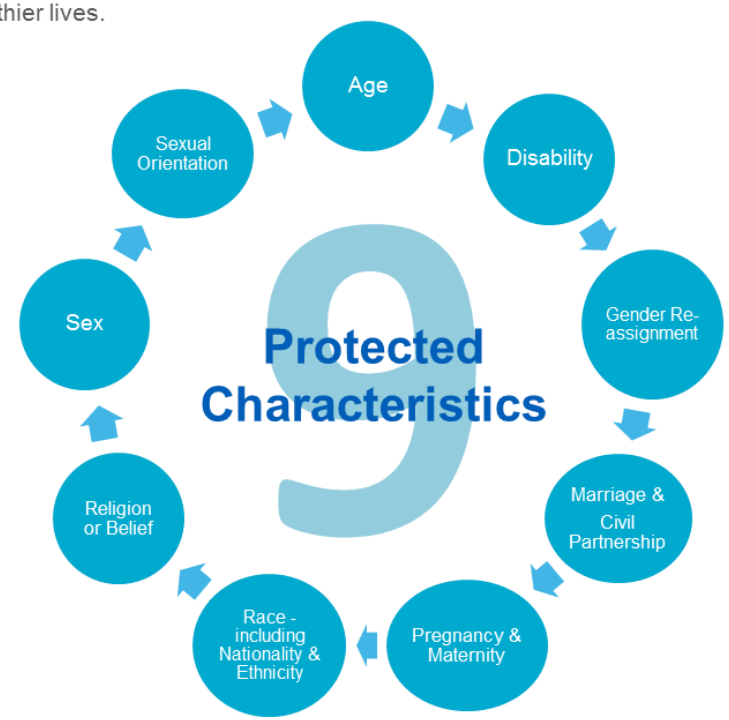
If the document upon assessment is identified as having a positive impact, how can this be shared to maximise the benefits universally?

Trust Equality and Diversity Objectives

Better health outcomes for all	Improved patient access & experience	Empowered engaged & included staff	Inclusive leadership at all levels

Our Vision

Working together with our partners in health and social care, we will deliver accessible, personalised and integrated services for local people whether at home, in the community or in hospital empowering people to lead independent and healthier lives.



Appendix C – Confidentiality Conditions for Clinical System Users

The following statements represent the confidentiality conditions of use for all users of clinical systems containing patient records:

- I understand that I am responsible for the security of my username and password. When I have received the password, I will ensure it remains secure and confidential, and will not disclose it to anyone at any time.
- I will not attempt to learn another person's password.
- I will never attempt to access information on the system by using any password other than my own or by any other unauthorised means.
- If I have reason to believe that the confidentiality of my password has been broken, I will report this immediately to my line manager and to the Trust IT Service Desk, in order that a new password can be assigned to me.
- I will never attempt to access or disclose any information without authority, and agree that, in the performance of all duties as an employee of Great Western Hospitals NHS Foundation Trust or as a user of its systems, I will abide by my legal obligation to hold all information in confidence in accordance with the Data Protection Act 2018.
- I understand that it is strictly forbidden for employees to look at any patient/employee information relating to themselves or their family, friends or acquaintances 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 in accordance with the Information Governance Policy.
- I understand that contravention of any of these conditions will lead to the Trust invoking the formal disciplinary procedure, and that any action taken against me may ultimately result in dismissal.

Appendix D – Clinical System Access Level Validation Form

Authorising Manager Name:	

A random clinical system audit has been undertaken by the Trust's Information Governance (IG) Team for the following personnel, in accordance with the Clinical Systems Access Monitoring & Audit Policy.

Audit Date:	
User Name:	
User's current access level:	

Caldicott principles for access to patient records:

1. *Justify the purpose.*
2. *Don't use patient identifiable information unless it is absolutely necessary.*
3. *Use the minimum necessary patient identifiable information.*
4. *Access to patient identifiable information should be on a strict need to know basis.*
5. *Everyone should be aware of their responsibilities.*
6. *Understand and comply with the law.*

According to our records you are the line Manager, or the Manager who authorised the IT access, for this employee /user. Please confirm that the current access level is appropriate and necessary to undertake activities directly concerned with, or in support of, the patients' healthcare, in compliance with local and national patient confidentiality initiatives.

To meet the terms of Caldicott principle 4, please verify that the group access provided above remains appropriate for the user's job role.

*** Please tick appropriate boxes:**

- ☐ The access level is appropriate for the user's current job role.
- ☐ The access level should be amended, please contact the IG Team to agree appropriate current access levels.

Authorising Manager name: (signed)		Authorising Manager name: (please print)	
Department:		Extension No.	
Bleep No.		Date:	
Email:			

Please return this completed form to the IG Team, Finance Dept, Commonhead Offices The Great Western Hospital, Marlborough Road, Swindon SN3 6BB.
Email: gwh.info.gov@nhs.net Tel: 01793 60(5675)

Appendix E – Audit Validation Form

Authorising Manager Name:	

A clinical system audit has been undertaken by Trust's Information Governance (IG) Team for the following personnel, in accordance with the Clinical Systems Access Monitoring & Audit Policy.

Audit Date:	
User Name:	

According to our records you are the line Manager, or the Manager who authorised the access to the system, for this member of staff/user.

As part of the audit review the following access details are considered:

- Were the details accessed for the patient within the employee's area of work?
- Has the employee undertaken any data changes outside of their recorded job remit?
- Has the employee accessed their own record, or the record of any likely family member?
- Has the employee repeatedly accessed the same patient record and/or remained in the patient record for a significant length of time that may or may not have been necessary as part of the patient's care or that could indicate a sharing of log-in details?

The attached audit has identified the following concerns (please also see highlighted report attached):

If you can confirm that the access would have been in order to undertake activities directly concerned with, or in support of, the patients' healthcare, in compliance with local and national patient confidentiality initiatives, please indicate this below. Otherwise the incident will be treated as a breach of confidentiality and will be investigated further in accordance with the Information Security Incident Reporting Procedure, potentially leading to disciplinary action.

*** Please tick appropriate boxes:**

☐ I confirm that the access to patient record(s) was appropriate and necessary and that further action will **not** be necessary.

☐ I agree with the identified concerns with the patient records accessed by the audited employee and I would like further investigations to be undertaken.

Authorising Manager name: (signed)				Authorising Manager name: (please print)	
Department:				Date:	
Extension No.		Bleep No.		Email:	

Please return this completed form to the IG Team, Finance Dept, Commonhead Offices, The Great Western Hospital, Marlborough Road, Swindon SN3 6BB.
Email: gwh.info.gov@nhs.net Tel: 01793 60(5675)