POLICY DOCUMENT

Burton Hospitals
NHS Foundation Trust

CONFIDENTIALITY POLICY

Approved by:	**Trust Executive Committee**
On:	**26 September 2017**
Review Date:	**August 2020**
Corporate / Directorate	**Corporate**
Clinical/Non Clinical	**Non Clinical**
Department Responsible for Review:	**Medical Director**
Distribution:	
• Essential Reading for:	**All Staff**
• Information for:	**All Staff**
Policy Number:	**41**
Version Number:	**11**
Signature:	
	Chief Executive
Date:	**26 September 2017**

Burton Hospitals NHS Foundation Trust

POLICY INDEX SHEET

Title:	**Confidentiality Policy**
Original Issue Date:	**February 2006**
Date of Last Review:	**August 2017**
Reason for amendment:	**Update following introduction of new process regarding sharing records**
Responsibility:	**Medical Director**
Stored:	**Trust Intranet**
Linked Trust Policies:	**Consent Policy** **Disciplinary Policy** **Fax Policy** **FOI-Handling Requests Policy** **Incident and Serious Incident Management Policy and Process** **Information Governance Policy** **Information Security Policy** **Records Management Policy** **Procedure for handling Subject Access Requests** **Whistleblowing Policy** **Social Media Policy**
E & D Impact Assessed	**222**
Consulted	**Information Governance Steering Group** **Medical Director/Caldicott Guardian** **Chief Nurse / Chief Operating Officer** **Deputy Chief Nurse** **Divisional Nurse Directors; Director of Human Resources** **Heads of Departments** **Divisional Medical Directors; Clinical Directors**

REVIEW AND AMENDMENT LOG

Version	Type of change	Date	Description of Change
7	Update	8.12.2011	
9	Update	28.02.16	
10	Update		Removal of reference to paper copies of forms and signposting people to log electronically via Datix
11	Review and update	August 2017	Inclusion of process and ability to log patient's requests to NOT share data with Third party providers e.g. Virgin Care

CONFIDENTIALITY POLICY

CONTENTS

Burton Hospitals NHS Foundation Trust

CONFIDENTIALITY POLICY

1. INTRODUCTION

All employees of Burton Hospitals NHS Foundation Trust (the Trust) have a twofold duty to patients and clients. The first is to do everything possible for their welfare and the second is to respect their confidence.

The need to ensure the confidentiality of information is, and always has been, a major concern of everyone working within the National Health Service (NHS).

However, keeping information confidential is not the same as keeping it secret. It is essential that relevant confidential information is available to those who have a need to know it in order to do their work. Balancing the need to keep information confidential with appropriate sharing may not always be straightforward.

2. POLICY STATEMENT

This Policy includes guidance for staff on processing information in accordance with the principles and legal obligations outlined in the Data Protection Act (1998) and how to comply with best practice for information handling as described in the NHS Code of Confidentiality and the Caldicott Report of 1997.

This Policy is intended to enable the Trust and its staff (including non-Trust staff with access to Trust information) to work effectively in a confidential manner for the benefit of users of our services. It should help protect patients/service users and staff from the misuse of their information and ensure that confidential information is handled in a lawful and appropriate manner by:

- Defining what is meant by the phrase “confidential information”
- Informing staff of their responsibilities in relation to such information
- Informing staff of the correct procedures for dealing with confidential information so that they do not inadvertently breach confidentiality
- Providing sources of further information.

3. EQUALITY AND DIVERSITY STATEMENT

This Policy applies to all staff contracted by the Trust. This includes, but is not limited to, staff on secondment to the Trust, students on placement, people working in a voluntary capacity and non-Trust staff with access to Trust information, irrespective of age, disability, race, nationality, ethnic origin, religion, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

This Policy has had an Equality Impact Assessment and is monitored in line with the review of the Policy.

4. COMPLIANCE WITH THE POLICY

All Trust employees and non-Trust employees who work within the Trust, or under contract to it, have a duty to maintain the confidentiality of information gained during their employment/association with the Trust. This includes, but is not limited to, staff on secondment to the Trust, students on placement, people working in a voluntary capacity, and non-Trust staff with access to Trust information. For convenience, the term 'staff' is used in this document to refer to all those to whom the Policy applies.

The duty of confidentiality arises out of common law, legal obligations, staff employment contracts and professional obligations.[1]

This duty continues after the staff member no longer works for/has an association with the Trust.

Any breaches of this duty including unauthorised breaches of confidentiality, inappropriate use of personal health records, or abuse of computer systems, will be treated as a disciplinary offence, which may result in staff employment, or association, with the Trust being terminated. It may also bring into question staff professional registration and possibly result in legal proceedings.

If staff have any questions contact their Line Manager, in the first instance, or the Caldicott office function for further information (contact details can be found under the Caldicott section on the intranet.
http://bhftintranet.burtonft.nhs.uk/Departments/caldicott/

5. MONITORING COMPLIANCE

The effectiveness of this Policy will be reviewed on an ongoing basis via the Information Governance Steering Group (IGSG) and the Caldicott office function. This will include Policy review and examination of confidentiality breaches and incident trends.

The Caldicott Officer will carry out spot checks on whether staff understand their responsibilities in regards to the issues surrounding the protection of confidentiality. The results of this monitoring will be reported to the IGSG.

If any shortfalls are identified further work will be undertaken by the Caldicott Officer to ensure effective communication to staff regarding their roles and responsibilities in respecting confidentiality. The resulting actions will be progressed and monitored by the IGSG, with any relevant issues being reported to the Trust Executive Committee.

6. DUTIES / ROLES AND RESPONSIBILITIES

The Trust

The Trust will ensure that patients upon entering the Trust will be made aware that the information they give will be recorded and may be shared in order to provide them with care and may be used to support local clinical audit and other work to monitor the quality of care provided.

[1] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

This will be done via the patient information booklet, leaflets sent with other communications, the Trust website and information contained on appointment letters etc.

The content of these communications will include:

- How the patient's information will be stored and used
- How their information may be shared, along with appropriate safeguards on confidentiality
- How their records will be kept secure
- How they may obtain access to their records
- How they may restrict the use and sharing of their information, if they so wish
- Where to find further guidance.

The Trust will ensure that the information is accessible by those patients with a range of special/different requirements.

Patients who require more detailed explanations should be guided towards a staff member who is able to answer their queries, e.g. PALS.

All Staff

All staff must ensure that they are aware of the requirements and standards of behaviour that apply.

The Caldicott Principles:

- Justify the purpose(s) - every proposed use or transfer of person identifiable information within or from an organisation should be clearly defined and scrutinised
- Don't use person-identifiable information (PID) unless it is absolutely necessary
- Use the minimum necessary PID
- Access to PID should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

All staff are responsible for reporting information incidents and near misses including breaches of confidentiality via the Datix system. Staff reporting a suspected breach of confidentiality are protected by the Trust's Policy for Whistleblowing – http://bhftintranet.burtonft.nhs.uk/Policies/whistleblowers-policy.html

Further information can be obtained from the Caldicott office function. Contact details can be found under the Caldicott section on the intranet. http://bhftintranet.burtonft.nhs.uk/Departments/caldicott/

All Managers

All managers are responsible for ensuring that the staff they manage are aware of this Policy and their individual responsibility for complying with it and what this means for them in their day to day work. For example, where to store information, acceptable email and internet use, not sharing passwords etc.

Managers will ensure that:

- Staff are up-to-date with their Information Governance mandatory training.
- Managers within their service area are aware of their responsibilities in relation to staff awareness
- Service/team specific procedures are in place to implement Trust policy where required
- The Information Governance Policy and process is adhered to and action taken to address non-compliance. If a confidentiality breach is suspected it is imperative that the incident is reported
- When staff leave, managers must inform the relevant people within the Trust so that their IT accounts/access to information systems can be disabled, ensure security passes, USB sticks, laptops, mobile phones etc. are returned
- Where necessary, other departments are informed of a potential Caldicott incident, e.g. HR, Risk or IT.

Information Governance Steering Group (IGSG)

The Trust's IGSG is responsible for overseeing the implementation of this Policy including monitoring compliance and ensuring that it is reviewed periodically.

Caldicott Guardian

The Caldicott Guardian is responsible for ensuring high standards of patient and personal information security and confidentiality are implemented throughout the Trust.

The Caldicott Guardian ensures that confidentiality is a Trust priority and relevant issues are represented at Board level.

Caldicott Officer

The Caldicott Officer's function is to support the Caldicott Guardian role and is responsible for IGSG reports, leading and supporting investigations, checking Trust compliance to the Policy. The Caldicott Officer will also ensure that where necessary, other departments are informed of any incidents, e.g. HR, Risk or IT.

7. CALDICOTT GUARDIAN

Caldicott Guardians were introduced in 1999 following a report commissioned for the Government by Dame Fiona Caldicott to review PID in the NHS. The report outlined the weaknesses in the way the NHS handled confidential data and made a number of recommendations including the appointment of Caldicott Guardians.

The Caldicott Guardian within the Trust is the Medical Director. It is their duty to ensure that patient data is kept secure and that all data flows internal and external are periodically checked against the Caldicott principles.

8. GUIDANCE

8.1 Confidentiality

8.1.1 What is Confidential Information?

Confidential information may be information about identifiable individuals including, but not limited to, patients/service users, carers, members of staff or other third parties. It may also be organisational information about the Trust or any other health or social care organisation.

It is not necessary for the name of the individual to be known for the information to be identifiable. For example, it may be possible to identify an individual when a number of data items are put together such as post code, ethnicity and medical condition.

Within the NHS, information about deceased people is not treated any differently to that of living people, that is, the duty of confidentiality extends beyond death.[2]

Confidential information may be in a variety of forms including but not limited to electronic, paper, digital or audio format, such as records, note books, message books, X-rays, photographs, audio tapes, voicemail etc, or it may be knowledge gained from overheard conversations or seeing someone sitting in a clinic waiting room.

Examples of confidential information the Trust holds include:

- Personal demographic details of patients/service users and staff
- Contact details of service users and staff
- Medical details of patients/service users and staff
- Ethnicity of service users and staff
- Bank and salary details of staff
- Results of Criminal Records Bureau checks
- Organisational financial information.

Information that has been placed in the public domain, except as a result of a breach of confidentiality, is not classed as confidential.

8.1.2 Why is Confidentiality Important?

Confidentiality is important to protect the privacy of all individuals (staff and patients) whose information the Trust holds.

Both staff and service users provide the Trust with confidential information about themselves. They have a legitimate expectation that the Trust will respect their privacy and treat their information appropriately.

In a service delivery setting it is important to maintain the trust of patients. Patients/service users entrust us with, or allow us to gather, confidential information relating to their health and other matters as part of seeking treatment. The trust uses this information to assess their needs and deliver appropriate treatment and care. It is essential that clinicians / practitioners have all relevant information to hand when treating or caring for people. If patients/service users do not trust the Trust with their information they may withhold vital information or not seek treatment.

In some circumstances, service users may lack the competence to extend this trust or may be unconscious, but this does not diminish the duty of confidence.

Trust is also important in managing health and safety and risk. Staff or patients may want to pass on information about other individuals, for example, to report poor practice/incidents/near misses. Staff should be aware of the appropriate procedures, which should be followed in such cases.

It is essential if the trust of staff and patients/service users is to be retained and legal requirements are to be met, that the NHS provides and is seen to provide a confidential service.

8.2 Staff Responsibilities

8.2.1 Inform Patients/Service Users/Staff about how we use their information

Being open and transparent with people about who you are, what your role is, why you are collecting information, how you will use it, who you may share it with and gaining consent is not only integral to processing information fairly under the Data Protection Act 1998 but is at the heart of addressing many issues around information sharing and confidentiality.

8.2.2 Record Information Accurately, Consistently and in a Timely Manner

Record information in accordance with Trust Policy and service specific procedures – see Records Management Policy for more information http://bhftintranet.burtonft.nhs.uk/Policies/records-management-policy.htm.

Staff have a duty to maintain accurate records. (This is vital to the provision of care and the running of the Trust).

If records are inaccurate, future decisions may be wrong and may result in harm to a service user or member of staff.

If information is recorded inconsistently, records will be harder to interpret resulting in delays and possible errors.

8.2.3 Disposal of Confidential Waste Appropriately

Confidential information may be stored in a number of formats such as paper records, information in notepads/message books, CDs/DVDs, hard drive of computers etc. All such information and devices storing confidential information must be disposed of appropriately and in line with Trust policy, for example, use of ‘confidential waste’ boxes, shredding, destruction of hard drives etc. See Records Management Policy

http://bhftintranet.burtonft.nhs.uk/Policies/records-management-policy.htm and/or the Information Security Policy for more information http://bhftintranet.burtonft.nhs.uk/Policies/information-security-policy.htm

8.2.4 Improve Standards of Practice wherever possible

In achieving best practice staff must:

- Be aware of the issues surrounding confidentiality, and seek training, support and advice as necessary in order to deal with them effectively
- Feedback comments or suggestions to managers on systems, procedures or working practices that give a cause for concern or could be improved
- Share good practice with colleagues (this is particularly important when poor practice is encountered)
- Report breaches, suspected breaches and near misses using the Trust's Governance reporting system Datix.

8.2.5 Use Social Networking Media appropriately

Social media is a collection of online communication channels that allow users to publicly create, share and interact with content and information as well as directly with other users. It is a powerful, instant way to connect and share with others and to join in with online communities and has many benefits if approached responsibly.

Social networking involves the building of online communities and networks encouraging collaboration and engagement.

Staff need to be aware of how to use social media appropriately with regard to confidentiality – please see the Trust Policy for more detail.
http://bhftintranet.burtonft.nhs.uk/Policies/employee-use-of-social-media-and-social-networking-policy.htm

8.2.6 Clinical Audit

For Clinical Audit, data should be anonymised wherever possible to protect personal data. This may be in the form of coding data or totally removing personal data from the audit. Advice and support should be sought from the Clinical Audit Team before using any data for clinical audit purposes. See the Clinical Audit area on the intranet for contact details.
http://bhftintranet.burtonft.nhs.uk/Policies/employee-use-of-social-media-and-social-networking-policy.htm

8.3 Consent

8.3.1 Consent to Obtain and Use information

See **section 8.2.1: Inform patients/service users/staff about how we use their information.**

It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, clinical governance and clinical audits, which are wholly proper components of healthcare

provision, might not be obvious to patients and should be drawn to their attention. Similarly, whilst patients may understand that information needs to be shared between members of care teams between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies.

Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and the Trust cannot assume that patients who seek healthcare are content for their information to be used in these ways.

Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

Where patients have been informed of:

- The use and disclosure of their information associated with their healthcare;
- The choices that they have and the implications of choosing to limit how information may be used or shared; then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that patients understand what may happen and are content, should be taken. Special attention should be paid to the issues around child consent (see point 8.3.3).

Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

There are situations where consent cannot be obtained for the use or disclosure of patient identifiable information, yet the public good of this use outweighs issues of privacy. Section 251 of NHS Act 2006 currently provides an interim power to ensure that PID, needed to support a range of important work such as clinical audit, record validation and research, can be used without the consent of patients (See **9.4** for more information).

For further information on the issues of Consent please consult the Consent Policy (http://queensintranet/Corporate/docs/Clinical/Consent_25.pdf).

8.3.2 Choosing to Opt Out

The Trust has a responsibility to ensure that those patients who do not wish their information to be shared with other third party providers (for example Virgin Care) are assured that their wishes will be adhered to. The Caldicott Office function will be responsible for this which will be monitored through IGSG. **Appendix 1** details screen-shots of this process

8.3.3 Consent: Capacity to Consent

Where an individual does not have the capacity to consent the responsibility for deciding the appropriate course of action lies with the agency giving care or the person with lasting power of attorney (LPA).

Where the agency giving care is responsible for decisions about information sharing, it must be made in the best interests of the patient/service user taking into consideration any previously expressed views of the client.

In accordance with the Mental Capacity Act 2005 (MCA) the agency, where appropriate, should consult other people, especially: anyone previously named by the patient as someone who should be consulted, carers, close relatives or friends of the patient, any attorney appointed under the MCA, the views of an appointed independent mental capacity advocate (IMCA), or any deputy appointed by the Court of Protection to make decisions for the patient.

8.3.4 Consent: Children and Young People

Young people of 16 years and older are presumed to be competent to give their own consent.

In the case of children and young people under the age of 16, consent is usually required from one person with parental responsibility (who is usually the mother or father or someone who holds a court order giving them parental responsibility).

Children under the age of 16 can give consent for themselves if they have sufficient understanding and intelligence to fully understand what is proposed, that is, they are Gillick/Fraser competent.

People with parental responsibility can authorise other people to make decisions about their children including the sharing of information.

8.4 Disclosing Personal Information

8.4.1 Legitimate Reasons for Disclosing Information

There may be a number of reasons where personal confidential information may be legitimately disclosed. For example:

- The patient/service user/staff member wishes the information to be disclosed
- Disclosure of the information is required for the purposes of providing care
- Disclosure is required by law, for example, by statute or court order
- There is an overriding public interest in disclosing the information.

If you are unsure for any reason please speak to your Line Manager in the first instance, Health Records Manager or Caldicott office function.

8.4.2 Rights of Individuals in relation to their information (including the right to access personal information)

Staff should understand and respect the rights of individuals in relation to their information. Under the Data Protection Act, individuals (known as data subjects) have certain rights about the way information about them is used, including the right to request information that is recorded about them in most cases. Please see/refer to The Procedure for Handling Subject Access Requests for more information http://bhftintranet.burtonft.nhs.uk/Departments/medical-records/Documents/BHFT-Subject-Access-Procedure.pdf

8.4.3 Dealing with requests for access to health records for deceased people

Applications to access the records of a deceased person are governed by the **Access to Health Records Act 1990.** Under this legislation where the patient has died, their personal representative, executor or administrator or anyone having a claim resulting from the death (this could be a relative or another person) has the right to apply for access to the deceased's health record. Please see/refer to The Procedure for Handling Subject Access Requests for more information http://bhftintranet.burtonft.nhs.uk/Departments/medical-records/Documents/BHFT-Subject-Access-Procedure.pdf

8.4.4 Reasons for Disclosing Information without Consent

There are circumstances when it is necessary to share information even though the individual has not consented. The reasons for not obtaining patient consent are varied and can include cases where gaining patient consent is not possible or even desirable if, for instance, the person is under criminal investigation.

These circumstances are the exception rather than the rule.

Information can be shared without the consent of the person whom the information is about when:

- It is in the public interest to do so[2]
- It is required by law.

Examples of sharing information in the public interest include:

- Where a child is believed to be at risk of harm (Children Act 1989).
- Where there is a risk of harm to anyone including the data subject.

[2] The public interest in sharing confidential information must be balanced against the public interest in maintaining a duty of confidentiality. Where that balance lies must be considered in each case, that is, the decision to disclose or withhold information must be made on a case by case basis.

- Where information is required for the prevention, detection or prosecution of a crime.

- Under the Mental Health Act 1983 where a service user objects to their 'nearest relative' being consulted re: -

    - An application for Treatment Order (Section 3) is being considered
    - An application for assessment and/or treatment in relation to the service user has been made
    - Under the Mental Health Act (Patients in the Community) Act 1995 where the service user is known to have the propensity to violent or dangerous behaviour

- Domestic Violence, Crime and Victims Act 2004 gives victims of specified sexual or violent offences the right to be informed of certain decisions if the offender becomes subject to provisions under the Mental Health Act 1983.

Examples of sharing information where it is required by law include:

- Notification of certain infectious diseases

- Where it is required by court order.

Confidential Information that is disclosed without Consent must follow the appropriate process (see 8.4.5).

8.4.5 Procedure for Disclosing Information without Consent

Disclosing patient information does not mean disclosing everything about that person. Disclosures should be proportionate and be limited to relevant details.

Each decision to disclose information must be considered on its own merit and decisions should take account of the individual circumstances of the case. Decisions will sometimes be finely balanced and staff may find it difficult to make a judgement, in which case they should seek advice from the Caldicott office function, either directly or via their Line Manager. It may be necessary for the organisation to seek legal or other specialist advice (e.g. from professional, regulatory or indemnifying bodies) or to await or seek a court order.

It may be necessary to justify such disclosures to the courts or to regulatory bodies. It is therefore important where information is shared without consent that the member of staff documents what information was released and when, to whom it was disclosed, and why it was felt justified. Likewise, it is important that decisions not to share information are also justified. Staff and/or the Trust can be held accountable for acts of omission as well as commission.

All non-consented disclosures and acts of omission must be documented in the patient notes and reported to the Caldicott office function for logging unless they are part of a delegated process, for example, Safeguarding Procedures.

8.4.6 Checklist of points that must be considered before disclosing confidential information

The purpose of these questions is to help staff decide the appropriate action to take if they are asked to disclose confidential information about a patient / member of staff. They are not sequential or definitive but are intended as a guide to good practice.

- Have I verified the applicant's identity?
- Is there a legitimate reason for disclosing the information?
- Is the information requested adequate, relevant and not excessive for the purpose?
- Do I have the authority to disclose the information?
- What is the most appropriate method of disclosing the information?
- Who do I need to inform that I have disclosed confidential information?
- What do I need to record about the request and disclosure/non-disclosure?
- Where do I record information about disclosure/non-disclosure?
- Do I need to report the disclosure/non-disclosure to anyone?

8.4.7 Verifying Identity

Staff must ensure that they can confirm the identity of the person and/or legitimacy of the organisation requesting information.

Requests in person
If staff are not familiar with the individual then they can ask for some photo identification.

Telephone requests
Staff can verify identity in the following ways:

- Telephone the individual back via the main switchboard of their organisation. If staff do not know the telephone number (for example, because it is an agency that they are not familiar with), then they should independently verify the number via a telephone directory/directory enquiry service, that is, don't accept the number as given by the applicant.

- Unless there is a local procedure in place that states otherwise, staff should ask for the request to be put in writing. All requests from the police should be put in writing.

Written requests
Written requests from organisations (for example, a solicitor or substance misuse agency) must be on headed notepaper. The address should be independently verified (that is, staff should not accept an address / fax number given to them for an organisation that you are unfamiliar with). The identity of the applicant should be verified for all written requests.

8.4.8 Disclosing information that is adequate, relevant and not excessive for the purpose

When disclosing information staff must consider:

- What does the recipient hope to achieve by the disclosure? (That is, what is the purpose of disclosing information?)
- What is the minimum amount of information you can share to achieve that purpose?
- Who does the information need to be shared with?

8.4.9 Appropriate methods of communicating confidential information (including safe haven procedures)

The most appropriate method of communicating information will depend on a number of factors including the sensitivity of the information, its destination and the urgency of the request. Information should be transferred effectively, that is, it should reach its destination in a timely manner, and securely. As a general rule, safe haven procedures must be followed (see **section 6.6 of the Information Security Policy** That is, staff should inform the intended recipient that they will be sending them confidential information and they should request acknowledgment of its receipt.

<u>By post</u>

- Ensure you have an up to date address for the intended recipient
- Confidential information should be addressed to a named individual or team and marked 'Private and confidential: for the addressee only'
- Confidential information sent in both the internal and external post should be in sealed envelopes or packaging
- Depending on the sensitivity of the information and where it is being sent to, information may be double or single wrapped and delivered by hand/recorded delivery/normal post/internal post - but not in a transit envelope (either sealed or unsealed)
- Information sent through the internal post should contain the name of the service and the work base address
- Information sent/transferred on portable media such as a DVD, CD rom or USB stick must be encrypted.

<u>By telephone</u>

- Ensure staff know the identity of the caller before giving out information (see 'verifying identity' above). Do not leave confidential information on voicemail.

By email

Staff must be careful when sending emails containing personal identifiable data(PID) or commercially sensitive information. The minimum information only should be sent (following Caldicott recommendations) and it should only be sent in the following circumstances:

- From one '@burtonft.nhs.uk' account to another, or one of the following addresses (secure within the Trust's internal network)

- @northstaffs.nhs.uk
  @ssotp.nhs.uk
  @sssft.nhs.uk
  @burtonft.nhs.uk
  @staffordshirecss.nhs.uk
  @stoke.nhs.uk
  @northstaffsccg.nhs.uk

- To any recipient of another NHS organisation or business partner via NHSmail accounts only. These addresses all end in '@nhs.net'. Both sender and recipient must use an NHSmail account (to obtain an NHSmail contact the IT service desk).
- Also it is permitted to send emails from @NHSmail to the following emails domains:

Department	Domains
Central Government	*.gsi.gov.uk *.gse.gov.uk *.gsx.gov.uk Note that @orgname.gov.uk is not secure
Police and Criminal Justice	*.pnn.police.uk *.scn.gov.uk *.cjsm.net
Local Government	*.gcsx.gov.uk
Defence	*.mod.uk

For more guidance please refer to section 5.10 Email User Policy of the Information Security Policy
http://bhftintranet.burtonft.nhs.uk/Policies/Information%20Security%20Policy.pdf

By text

- Confidential or sensitive information must not be sent by SMS text message.

8.4.10 Informing appropriate individuals that confidential information has been disclosed

The patient/service user/staff member

- Even where there are grounds for disclosing confidential information without consent it is good practice to ask permission to do so

- Where a patient/service user/staff member has disclosed information that staff feel needs to be disclosed to a third party, it may be appropriate to give the patient/staff member an opportunity to disclose this information him/herself first. Staff should follow this up later, by an agreed date with the individual, to ensure the information has been disclosed

- If it is decided that it is necessary to disclose information even though the patient/service user/staff member has specifically withheld their consent, it is good practice to inform him/her

- The patient/service user/staff member should not be asked for permission to release information or told that information about them has been disclosed without their consent if it would prejudice the investigation of a crime or would put any individual at risk of harm.

Other Health and Social Care Professionals

- It is important to identify and inform any individuals who need to be made aware that confidential patient/service user/staff member information has been disclosed. This is particularly important where information has been disclosed without consent.

8.5 Information Security

For more information please see the Information Security Policy.
http://bhftintranet.burtonft.nhs.uk/Policies/Information%20Security%20Policy.pdf

8.5.1 Confidentiality in Public Places

Be aware of the difficulties of maintaining confidentiality in open plan offices.

Do not discuss confidential information in public areas where it may be overheard, for example:

- In corridors, reception areas, when using mobile phones, etc.

- Do not record confidential information where it may be accessed by unauthorised people – for example, on white boards, card systems that are not locked away, etc.

8.5.2 Access to information

- Do not browse electronic systems or records

- Do not access information which staff do not have a need to know

- Do not access records pertaining to yourself, your family, your friends or colleagues

- Ensure confidential information stored in a shared drive is accessible only to those with a need to know

- Consider how PC screens are positioned. Can confidential information be seen by anyone who does not have a need to know?

- Do not leave confidential information unattended, for example, do not leave information out on a desk or leave the desk when logged onto information systems

- Ensure paper records or (PID) is shredded and/or disposed of in confidential waste when no longer required

- **Lock your work station** even when you are away from your desk for short periods such as to make a cup of tea or take a comfort break

- Share information on a need to know basis

- Do not access the computer using another's log on, nor allow anyone to use your log on.

8.5.3 Passwords

Use passwords to access electronic systems in line with Trust's Information Security Policy, for example, in deciding what the password should be, how often it is changed, not sharing passwords, locking workstations, password protecting documents etc. In particular staff must ensure they;

- Do not share passwords with others

- Change passwords at regular intervals

- Do not re-use old passwords

- Do not write passwords down in a way that would allow another to access it/use it to access accounts

- Avoid using short passwords or using names or words that are associated with them, for example, children's or pet's names

- Use a combination of numbers, letters (upper and lower case) and characters.

8.6 Freedom of Information Act

Under the Freedom of Information Act 2000 (FOI), individuals can request access to any information the Trust holds. The Trust is legally obliged to provide a response, including any disclosable information, within 20 working days (see FOI Intranet page for more information. for more information.

http://bhftintranet.burtonft.nhs.uk/Departments/Governance/Freedom-of-Information/

The Caldicott principles still apply to these requests.

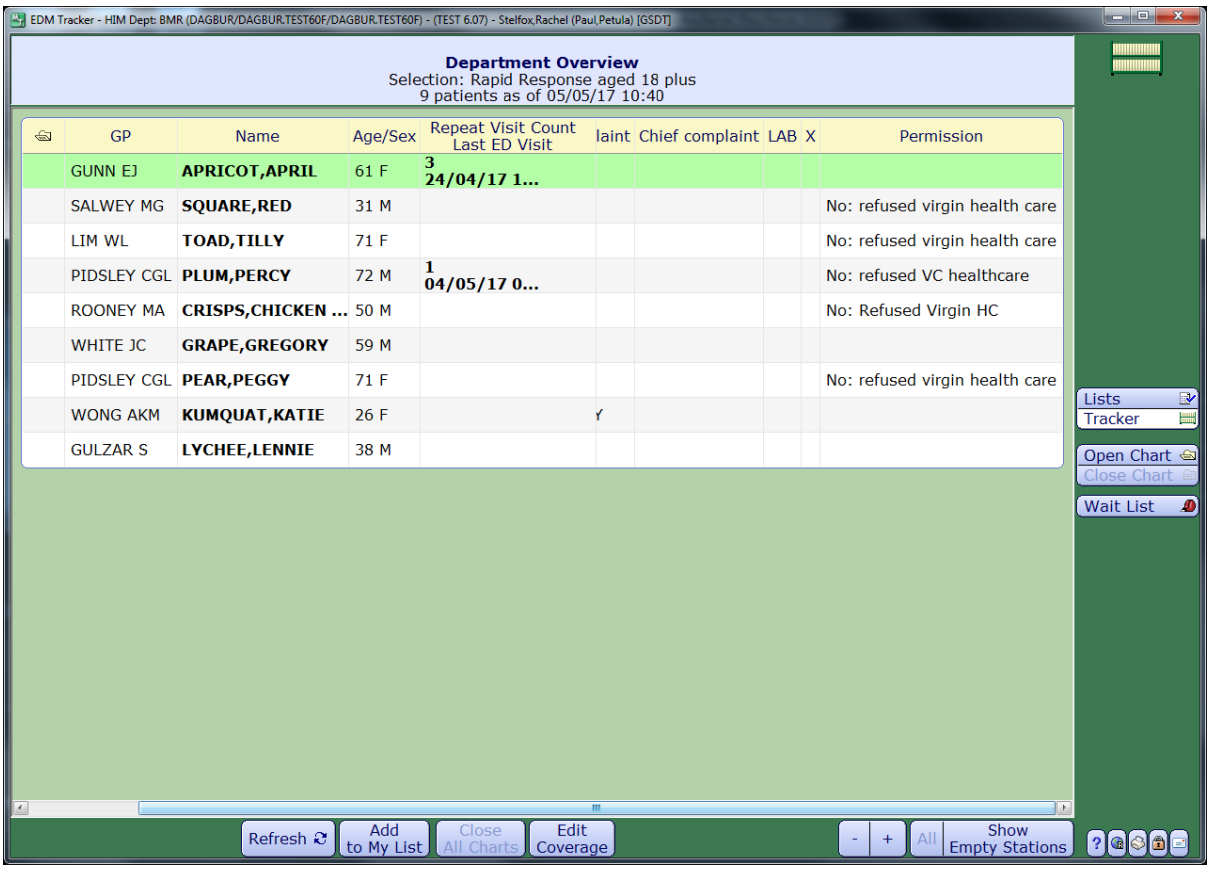
9. REFERENCES

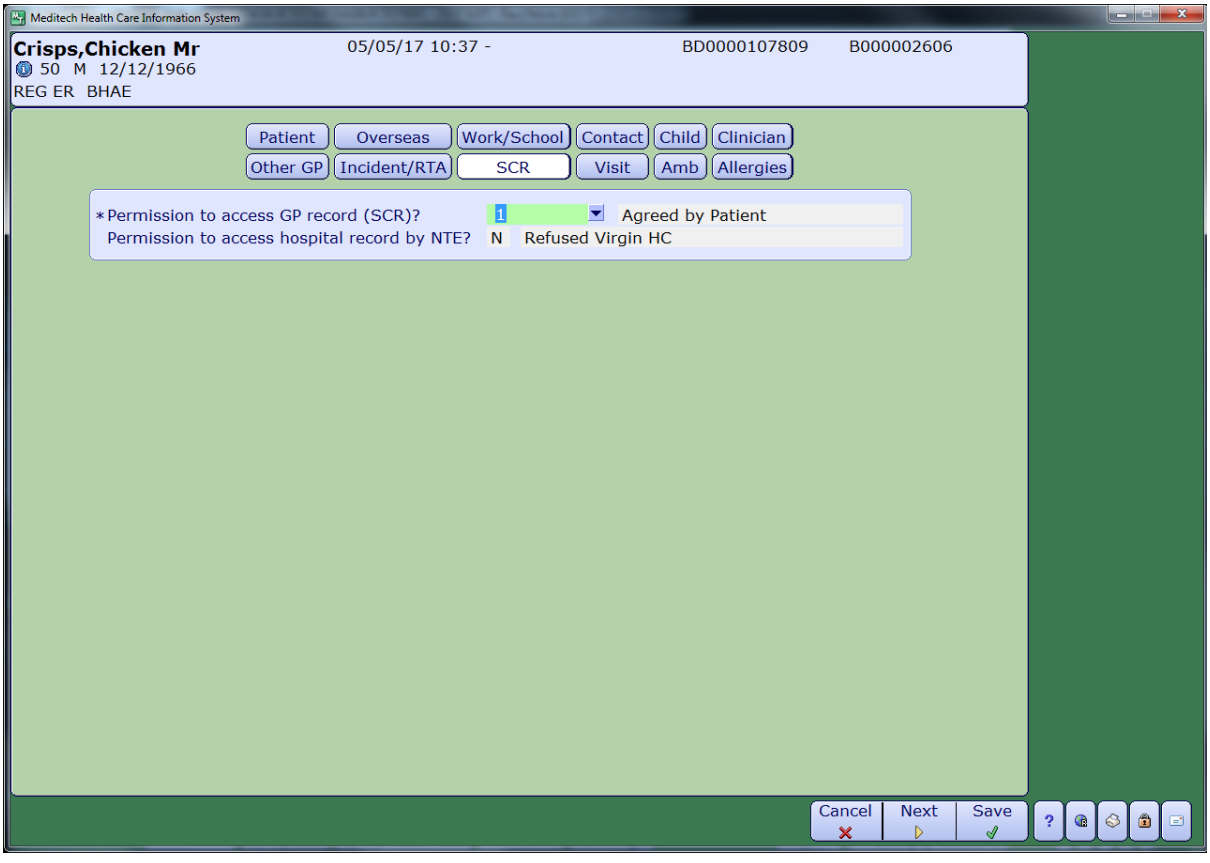
For this Policy the following references apply:

Data Protection Act 1998
Common Law Duty of Confidentiality
NHS Confidentiality Code of Practice

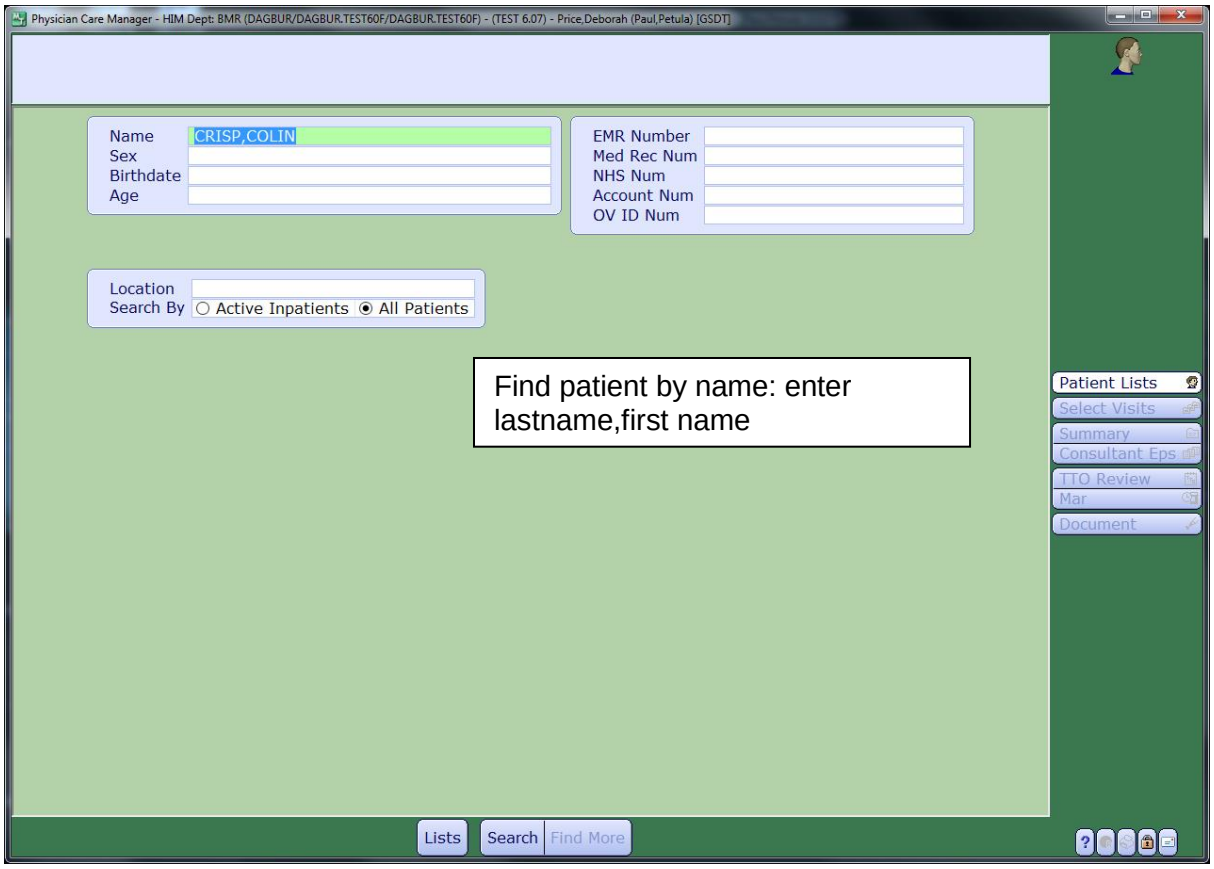
Freedom of Information Act 2000
The Caldicott Manual, 2010
New external IG training material will be available on the e-L-H website (not yet launched)

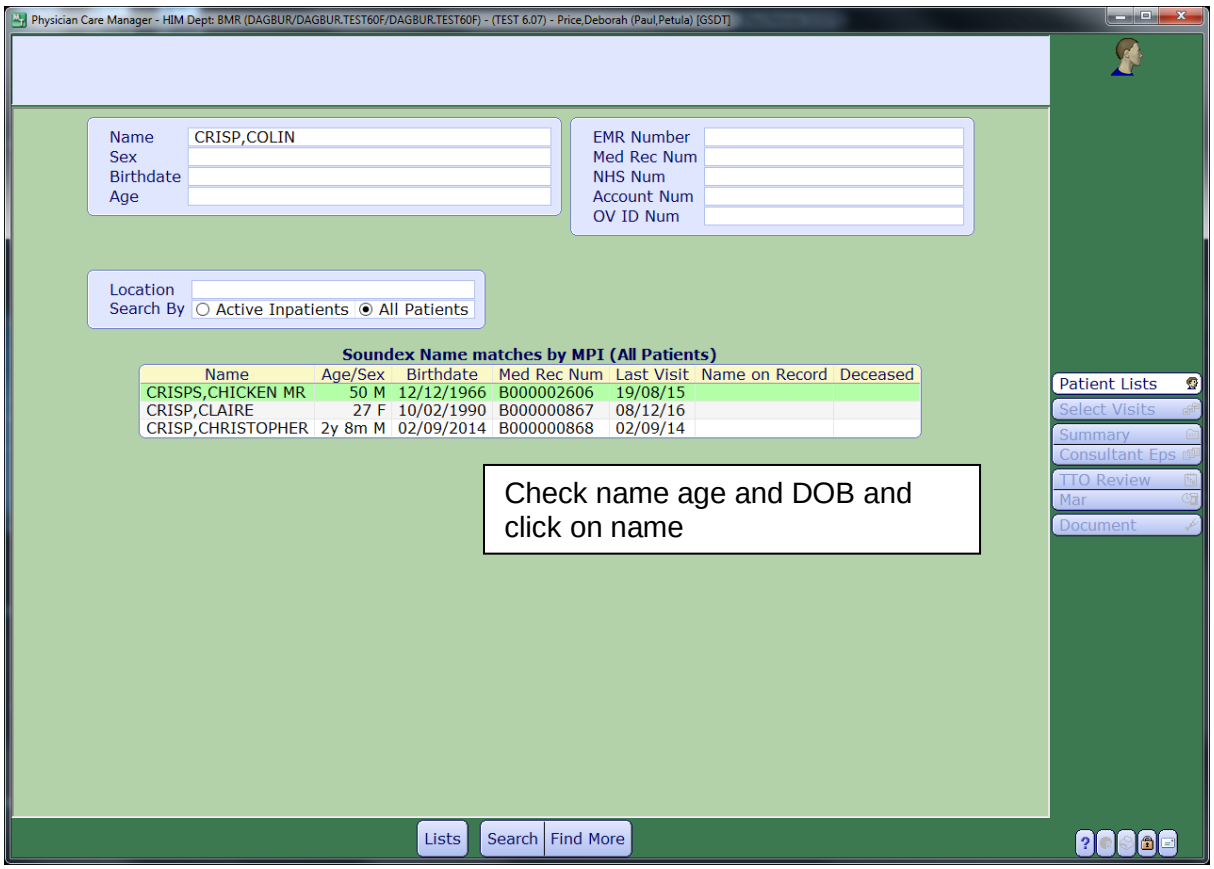
Caldicott Permissions for end users

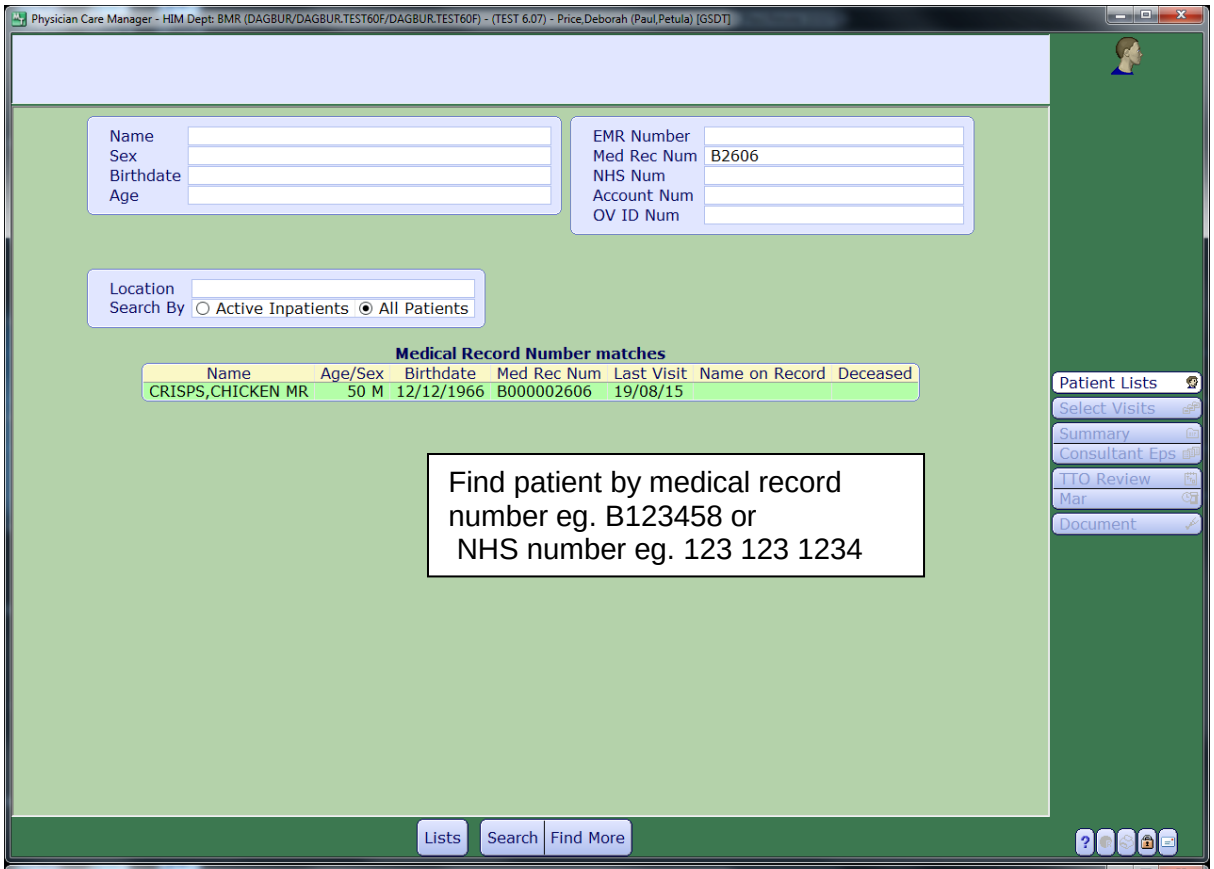


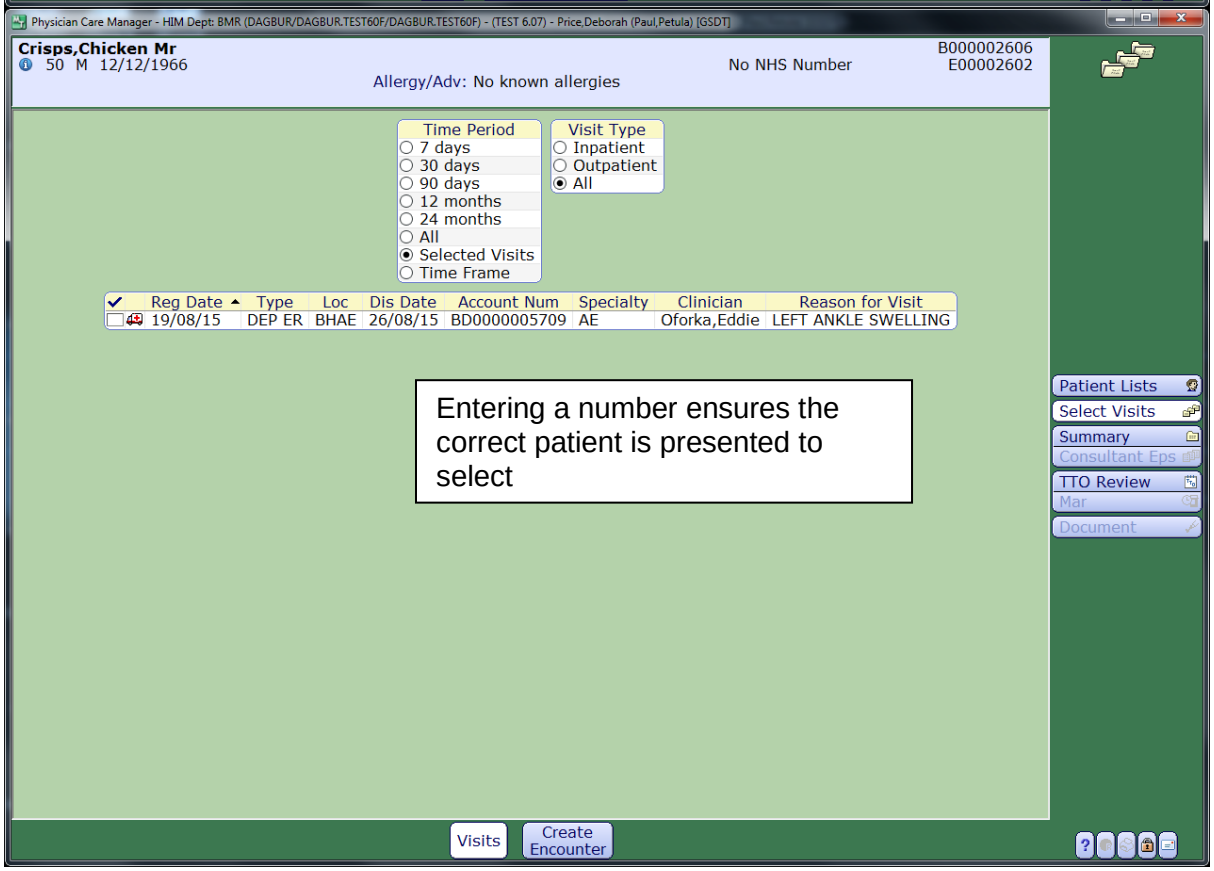


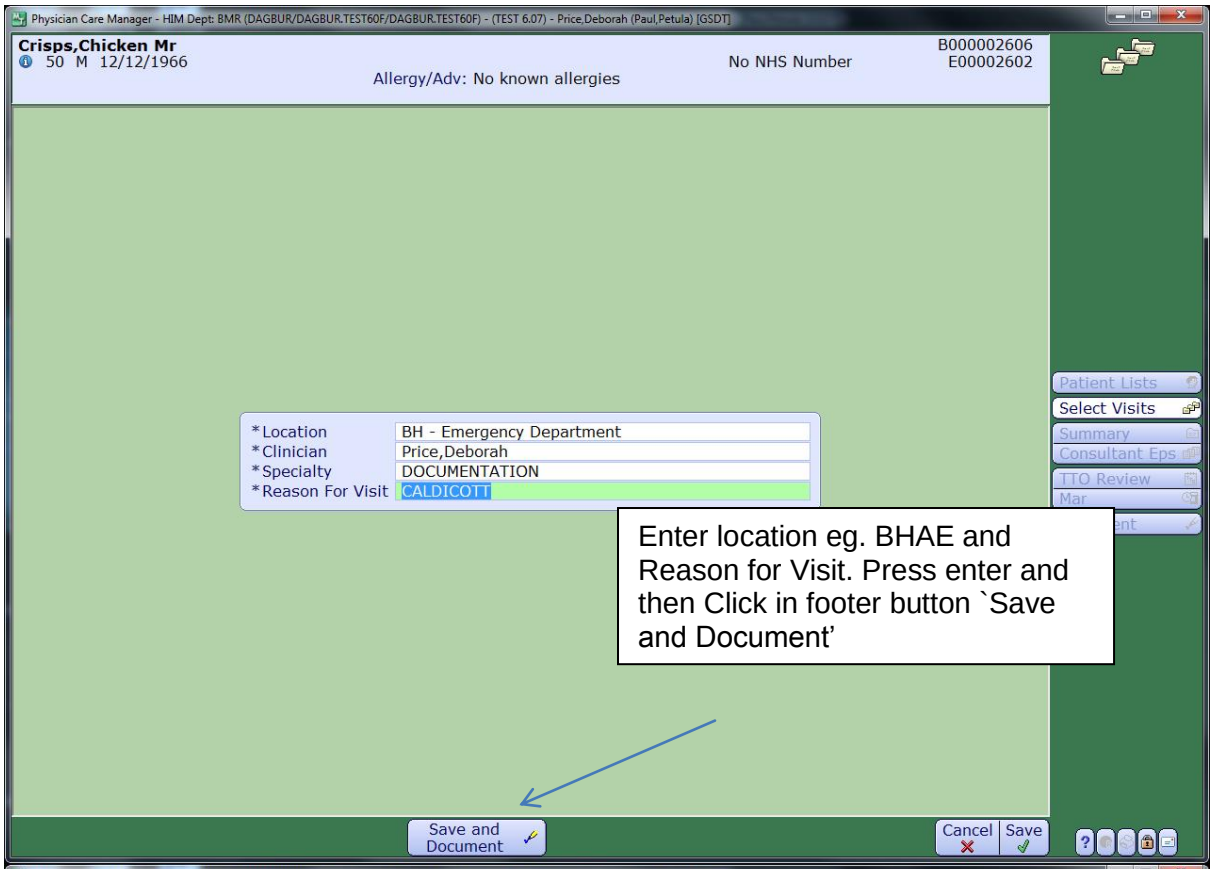
Version 6.0 Caldicott Recording permission

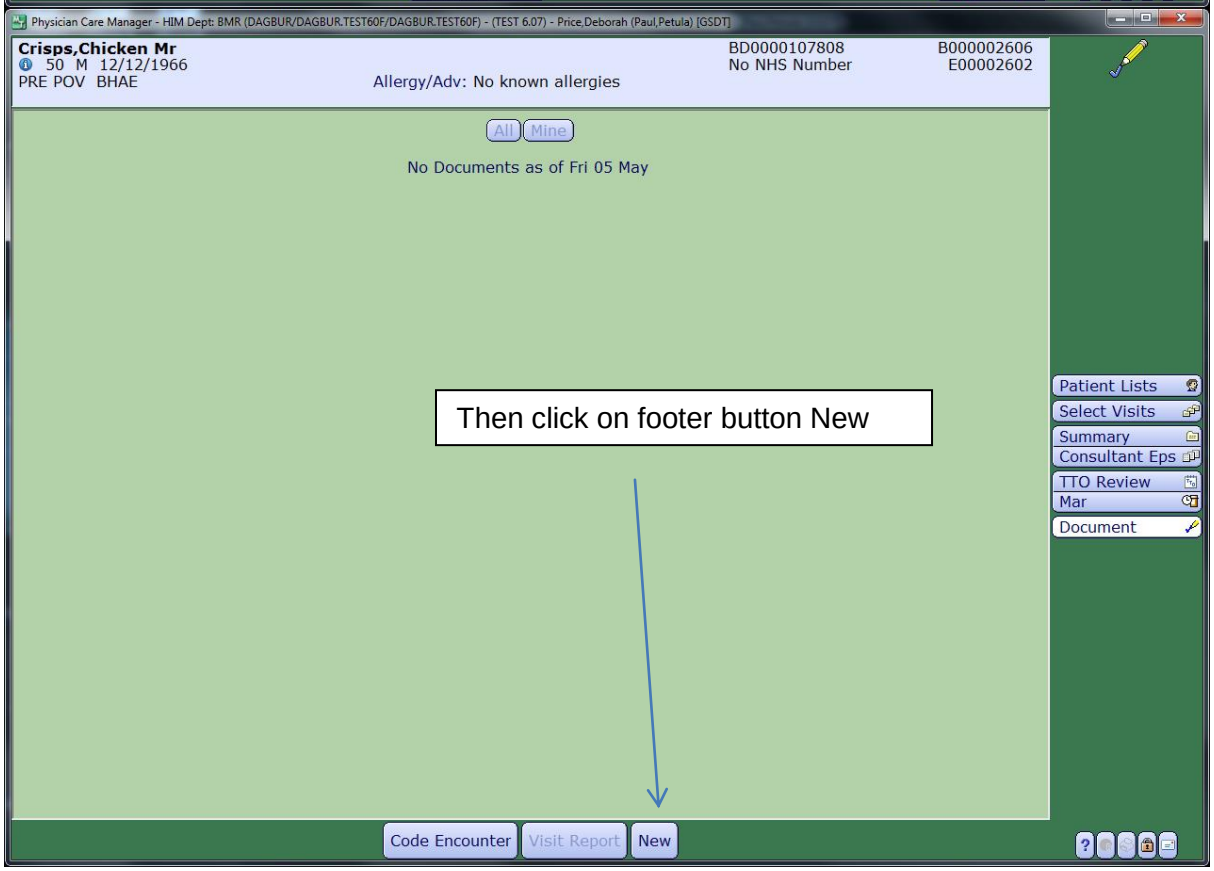

Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Name CRISP,COLIN
Sex
Birthdate
Age
EMR Number
Med Rec Num
NHS Num
Account Num
OV ID Num
Location
Search By Active Inpatients All Patients
Find patient by name: enter lastname,first name
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Lists
Search
Find More

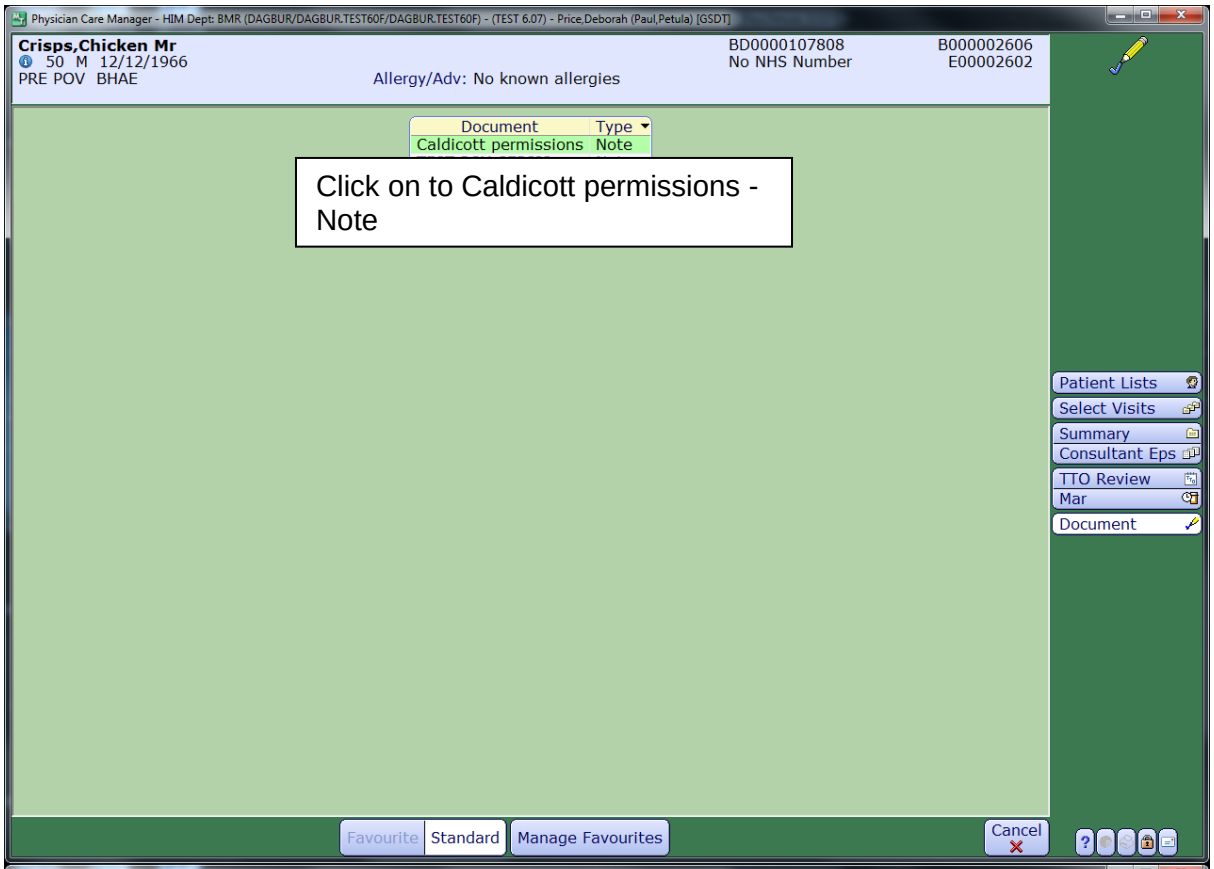

Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Name CRISP,COLIN
Sex
Birthdate
Age
EMR Number
Med Rec Num
NHS Num
Account Num
OV ID Num
Location
Search By Active Inpatients All Patients
Soundex Name matches by MPI (All Patients)
Name Age/Sex Birthdate Med Rec Num Last Visit Name on Record Deceased
CRISPS,CHICKEN MR 50 M 12/12/1966 B000002606 19/08/15
CRISP,CLAIRE 27 F 10/02/1990 B000000867 08/12/16
CRISP,CHRISTOPHER 2y 8m M 02/09/2014 B000000868 02/09/14
Check name age and DOB and click on name
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Lists
Search
Find More

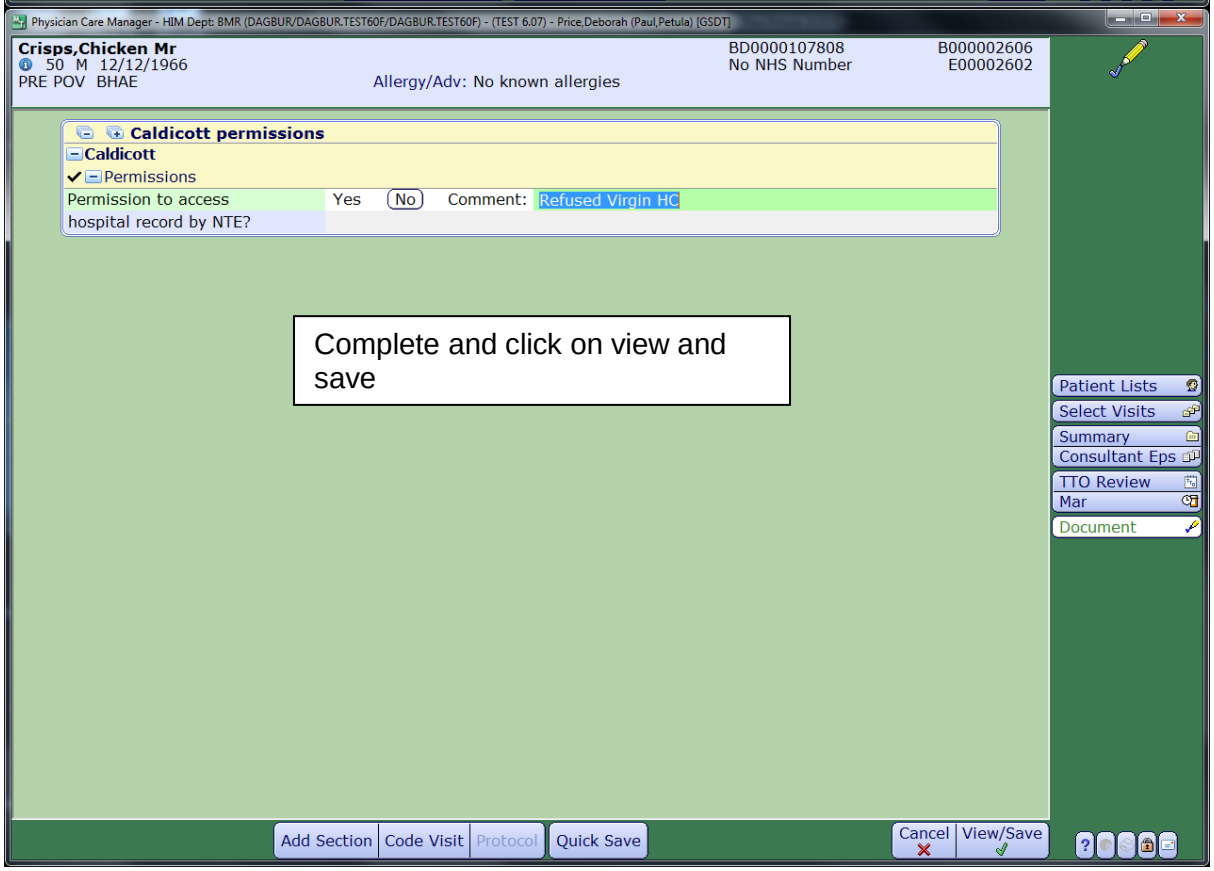

Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Name
Sex
Birthdate
Age
EMR Number
Med Rec Num B2606
NHS Num
Account Num
OV ID Num
Location
Search By Active Inpatients All Patients
Medical Record Number matches
Name Age/Sex Birthdate Med Rec Num Last Visit Name on Record Deceased
CRISPS,CHICKEN MR 50 M 12/12/1966 B000002606 19/08/15
Find patient by medical record number eg. B123458 or NHS number eg. 123 123 1234
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Lists
Search
Find More

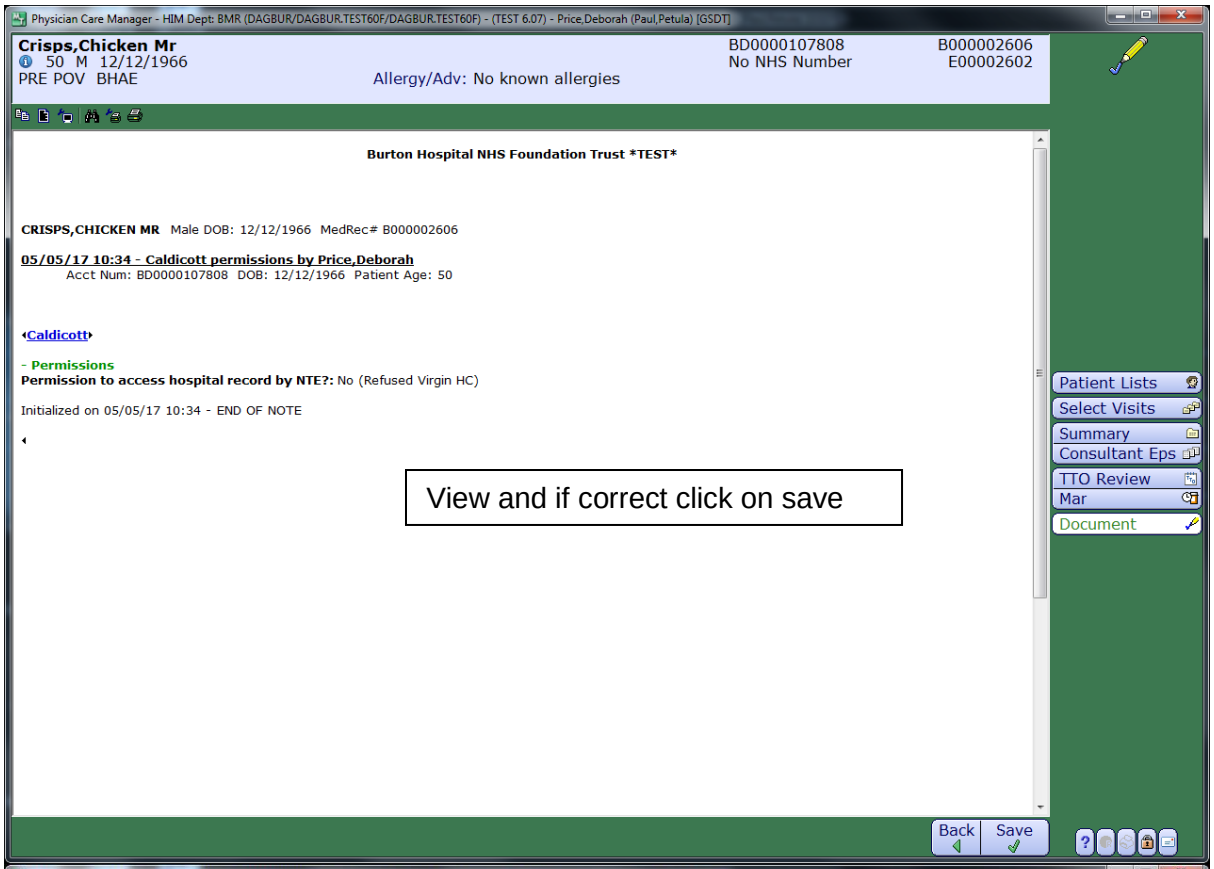

Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
Allergy/Adv: No known allergies
No NHS Number
B000002606
E00002602
Time Period
7 days
30 days
90 days
12 months
24 months
All
Selected Visits
Time Frame
Visit Type
Inpatient
Outpatient
All
Reg Date Type Loc Dis Date Account Num Specialty Clinician Reason for Visit
19/08/15 DEP ER BHAE 26/08/15 BD0000005709 AE Oforka,Eddie LEFT ANKLE SWELLING
Entering a number ensures the correct patient is presented to select
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Visits
Create Encounter


Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
Allergy/Adv: No known allergies
No NHS Number
B000002606
E00002602
*Location
BH - Emergency Department
*Clinician
Price,Deborah
*Specialty
DOCUMENTATION
*Reason For Visit
CALDICOTT
Enter location eg. BHAE and Reason for Visit. Press enter and then Click in footer button `Save and Document'
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Save and Document
Cancel
Save

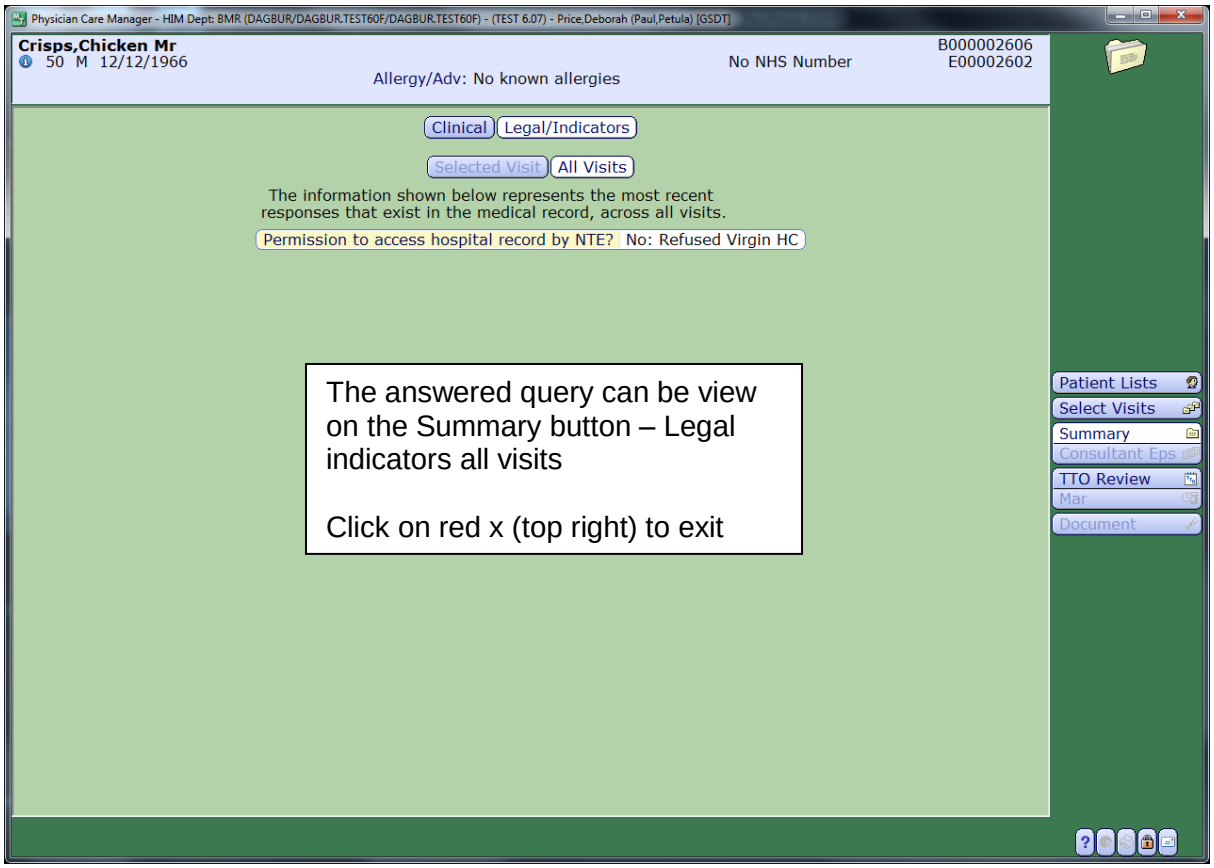

Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
PRE POV BHAE
Allergy/Adv: No known allergies
BD0000107808
No NHS Number
B000002606
E00002602
All
Mine
No Documents as of Fri 05 May
Then click on footer button New
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Code Encounter
Visit Report
New


Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
PRE POV BHAE
Allergy/Adv: No known allergies
BD0000107808
No NHS Number
B000002606
E00002602
Document
Type
Caldicott permissions
Note
Click on to Caldicott permissions - Note
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Favourite
Standard
Manage Favourites
Cancel


Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
PRE POV BHAE
Allergy/Adv: No known allergies
BD0000107808
No NHS Number
B000002606
E00002602
Caldicott permissions
Caldicott
Permissions
Permission to access hospital record by NTE?
Yes
No
Comment:
Refused Virgin HC
Complete and click on view and save
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Add Section
Code Visit
Protocol
Quick Save
Cancel
View/Save


Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
PRE POV BHAE
Allergy/Adv: No known allergies
BD0000107808
No NHS Number
B000002606
E00002602
Burton Hospital NHS Foundation Trust *TEST*
CRISPS,CHICKEN MR Male DOB: 12/12/1966 MedRec# B000002606
05/05/17 10:34 - Caldicott permissions by Price,Deborah
Acct Num: BD0000107808 DOB: 12/12/1966 Patient Age: 50
‹Caldicott›
- Permissions
Permission to access hospital record by NTE?: No (Refused Virgin HC)
Initialized on 05/05/17 10:34 - END OF NOTE
‹
View and if correct click on save
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Back
Save


Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
PRE POV BHAE
Allergy/Adv: No known allergies
BD0000107808
No NHS Number
B000002606
E00002602
All
Mine
No Documents as of Fri 05 May
The note does not display on this screen
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document
Code Encounter
Visit Report
New


Physician Care Manager - HIM Dept: BMR (DAGBUR/DAGBUR.TEST60F/DAGBUR.TEST60F) - (TEST 6.07) - Price,Deborah (Paul,Petula) [GSDT]
Crisps,Chicken Mr
50 M 12/12/1966
No NHS Number
B000002606
E00002602
Allergy/Adv: No known allergies
Clinical
Legal/Indicators
Selected Visit
All Visits
The information shown below represents the most recent responses that exist in the medical record, across all visits.
Permission to access hospital record by NTE? No: Refused Virgin HC
The answered query can be view on the Summary button – Legal indicators all visits
Click on red x (top right) to exit
Patient Lists
Select Visits
Summary
Consultant Eps
TTO Review
Mar
Document