Reference Number: UHB 376 **Version Number:** 1	**Date of Next Review:** 17th Oct 2017 **Previous Trust/LHB Reference Number:** N/A

Guidance On Completing Data Protection Permissions Coordinating Process Governance Checks

Introduction and Aim

As part of the Health and Care Research Wales Permissions Coordinating Process a governance review is completed for each research application. This review includes checks to ensure compliance with data protection requirements. Traditionally, these checks have been completed by the CVUHB Data Protection Manager (DPM). It has been agreed that R&D Office staff will now undertake these checks on behalf of the DPM. However, overall responsibility for the governance checks lies with the DPM.

Where R&D staff have any concerns regarding completing data protection checks for a study, it should be referred to the DPM for review/advice.

The DPM will maintain oversight of completed reviews by randomly selecting studies which have been reviewed by the R&D Office and completing a second review. Projects will be selected from the monthly CaRRS Scoring Sheet document. Any issues will be addressed as necessary.

Objectives

- To ensure compliance with data protection requirements

Scope

This procedure applies to all of our staff in all locations including those with honorary contracts.

Equality Health Impact Assessment	An Equality Health Impact Assessment (EHIA) has not been completed. 'This is because a procedure has been written to support the implementation of the Research Governance Policy. The Equality Impact Assessment completed for the policy found here to be no impact.
Documents to read alongside this Procedure	
Approved by	Research Governance Group

Accountable Executive or Clinical Board Director	Medical Director
Author(s)	Registrations and Permissions Improvement Manager

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date of Review Approved	Date Published	Summary of Amendments
1	17/10/17	13/12/17	New Procedure

1. GOVERNANCE CHECKS

This section details those checks which require consideration from a data protection perspective. A summary of each check is provided, followed by tables which give details of how to complete the checks.

Studies should comply with the Data Protection Principles:

1. Personal data must be fairly and lawfully processed
    a. Why is information being collected; what will be done with it; with whom it will be shared?

2. Personal information must be processed for limited purposes
    a. Only use personal information for the purpose for which it was obtained

3. Personal information must be adequate, relevant and not excessive
    a. Only collect the information required, It is not acceptable to hold information without a view as to how it will be handled.

4. Personal information must be accurate and up to date
    a. Checks should be in place to ensure information has been recorded accurately and is up-to-date. If it isn't written down, it didn't happen

5. Personal information must not be kept for longer than necessary
    a. Ensure regular disposal of information; do not keep it because it may be useful one day;

6. Personal information must be processed in line with the data subjects' rights
    a. Individuals have the right to request to see information held about them; to request correction of any information they feel is incorrect; ensure their information is kept confidentially

7. Personal information must be secure
    a. Appropriate physical and electronic security must be in place to ensure confidentiality

8. Personal information must not be transferred to other countries without adequate protection.
    a. Do not transfer information outside of the EAA without first checking with the Information Governance department

There is an absolute exemption in the Freedom of Information Act (section 40(1)) to requesting your own personal data. The Data Protection Act 1998 must be used for this.

Where research is being undertaken through independent contractors, it is the independent contractor's responsibility to ensure that arrangements meet local policies and standards. Independent contractors may seek advice to meet their responsibilities.
Data protection governance checks focus on two main areas: the participant information/consent documents and process, and compliance with the Data Protection Act 1998 and data security issues.

Participant information /consent documents and consent process

Note: Study-wide checks are completed by the R&D Office for single-NHS organisation studies and are completed by the Health and Care Research Wales Permissions Service for multi-NHS organisation studies. Local checks are completed by the R&D Office for all studies.

Check 2.1: Study-wide check
This check reviews risk to participants and how this is minimised by providing accurate information on the research to potential participants and ensuring that any legislation relating to the research is followed.

Potential participants in any study need information upon which to base their decision whether to take part. Participant information sheets and consent forms are only part of the information given to potential participants during the informed consent process. The

process of seeking informed consent also involves a discussion between members of the research team and the potential participant. The potential participant may also have discussions with an independent person e.g. family member, GP. Where Participant Identifications Centres are to be used there should be a clear process for providing information to potential participants and who is responsible for the consent process.

Research ethics committees consider the ethical implications of the information provided to potential participants, and of the consent process, where relevant. NHS organisations need to be assured that potential participants receive accurate information on the research and that any legislation relating to that research is followed.

Review the protocol and IRAS form A27 - A31 to check that the consent process is appropriate and complies with legislation.

Check C2: Local check
This check reviews whether any legal implications in the consent process have been highlighted and addressed.

Potential participants in any study need information upon which to base their choice to take part. Information sheets and consent forms are only one part of the process of seeking informed consent. The Health Research Authority (HRA) provides guidance on information sheets and consent forms. It advises that the length and level of detail in any information sheet should take account of the complexity and risk of the research. Where appropriate, the information sheet may be divided into two parts. The REC will only consider the ethical implications of the information provided to potential participants, and of the consent process. NHS organisations have a duty to ensure participants receive accurate information on the research that may affect their care, and for ensuring any legislation relating to that research is followed.

Compliance with Data Protection Act and data security issues assessed

Check 5.1: Study-wide check
This check reviews legal compliance with the Data Protection Act 1998, Human Rights Act 1998 and obligation of confidentiality in common law. The use of a patient's data is covered by a large range of legal and professional obligations. There are also a number of statutes that describe how a patient's data may be disclosed and used.

NHS organisations are expected to protect the way identifiable data is handled in accordance with the Data Protection Act 1998, ensure privacy is maintained in accordance with the Human Rights Act 1998 and satisfy the obligation of confidentiality in common law. Under common law all research using identifiable patient data requires the express (explicit) consent of the patients involved or another legal basis. In certain circumstances, and with the necessary approvals, the common law duty of confidentiality may be set aside so that information that identifies patients can be used without their consent.

It is important to note the difference between:

- "personal data" (data relating to a participant who could be identified from that data) IRAS form A36 – A40 and A43
- "research data" (data generated from the study which is anonymised and from which participants could not be identified) IRAS form A44 - A45.

Check C16: Local check

This check reviews legal compliance with the Data Protection Act 1998, Human Rights Act 1998 and obligation of confidentiality in common law. It assesses whether access to and handling of personal identifiable data is in line with the organisation's policies.

There are a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

NHS organisations must protect the way identifiable information is handled in accordance with the Data Protection Act 1998, ensure privacy is maintained in accordance with the Human Rights Act 1998 and satisfy the common-law duty of confidentiality. Those who work within or under contract to NHS organisations are expected to comply with NHS-specific codes of practice and to demonstrate high standards of information governance.

The Access to Health Records Act 1990 does not provide a legal basis for next of kin to consent to the review of medical information of deceased patients. Confidentiality Advisory Group (CASG) approval may be needed.

Check	Questions	Notes for completion
2.1	Are patient or service user records being used to identify potential participants?	Normally only a member of the patient's existing clinical care team should have access to patient records without explicit consent in order to identify potential participants. Patient or service user records may legally be used to identify potential participants by fulfilling any of the following criteria: ▪ The researcher gains the explicit consent of every patient with a record in the population pool being assessed ▪ The search is conducted by a health or social care professional who has a 'legitimate relationship' with the patient, such as a clinical or social worker ▪ The search is conducted by a researcher who is part of the clinical team ▪ The search makes use of 'privacy enhancing technologies' ▪ Support under section 251 regulations is granted for the research (in England and Wales)
2.1	Who is making the initial approach to potential participants?	Initial identification and approach must be made by members of the clinical care team. Normally only a member of the patient's existing clinical care team should have access to patient records without explicit consent in order to make the initial approach to patients. If the research proposes to use someone outside the clinical team to identify suitable participants or as first contact with the participant, the reason for this should be explained in IRAS Form A27 – A29. For the purposes of research, Health and Care Research Wales workforce staff (or

Check	Questions	Notes for completion
		similarly UHB employed individuals) are considered to be part of the patient's clinical care team because they are providing assistance to the clinical care team and have a legitimate. As such, they have legitimate reason to access patient notes, make initial contact with the participant etc.
2.1	Are staff participants appropriately identified?	
2.1	Will consent by obtained and recorded in writing?	Generally, a participant should be given a minimum of 24 hours to make a decision whether to participate in a study. Consent is generally not required if the only research procedure is completion of a questionnaire. In this case completing the questionnaire implies consent. If consent will not be obtained/recorded, IRAS A30-1 should explain why not.
2.1	Does the study involve adults with mental capacity issues?	If incapacitated participants are involved in a non CTIMP study is the consent process compliant with the Mental Capacity Act? For CTIMPS, the CT regulations must be followed and this will be covered in check 5.2

2.1	Is consent obtained for all relevant items?	• Consent form should include consent for:
		  • tissue samples to be taken,
		  • tissue/data to leave the UK/Europe,
		  • audio or video recordings to be made,
		  • quotes to be published,
		  • pictures to be taken ,

Check	Questions	Notes for completion
		• access to medical records by ….. • storage of personal data • any other activity which could compromise confidentiality or lead to identification of the participant • must have initial boxes, not tick boxes • if patient medical records are being accessed as part of the study, consent must be obtained • if the patient's GP is being informed of participation, this requires consent • all key parts of the study relating to the processing of patient data (disclosures, future use of data) require consent • if researchers may wish to contact participants for subsequent studies, the participant should be informed and consent obtained • The consent form should refer to PIS date/version… Ensure the correct details are in the consent form
2.1	Is the information in the PIS and ICF accurate?	• Does the PIS: • State it is a student study in the first paragraph, if applicable • Provide brief clear information on the essential elements of the study • Provide information on the condition or treatment under study, if applicable • Describe the voluntary nature of taking part • Describe what will happen during and after the study • Describe the participant's responsibilities • Describe the potential risks, inconveniences and benefits

Check	Questions	Notes for completion
		• Explain disclosure i.e. confidentiality may be broken any of the following are identified: malpractice by staff, evidence of harm to participants/patients, incidents relevant to the criminal justice system, adverse effects on wellbeing/health. It may be necessary to request information on the procedure for this. • information relating to insurance/indemnity (if applicable) • information on funding, concerns/complaints and data protection arrangements • Does the consent form have separate statements for: • Photographs • Quotes • Audio or video taping • Any other activity which could compromise confidentiality or lead to identification of the participant • Sampling (if applicable e.g. blood sample ref staff vaccination) • The PIS should include a confidentiality section and should detail the use of personal data. The information should tally with the protocol. Confidentiality should cover (in general terms) what is disclosed, to whom, what security is applied, any further uses/disclosures of data. • Collecting both initials and D.O.B. makes it possible that the participant could be

Check	Questions	Notes for completion
		identified. The researcher needs to justify the reason for this data collection. If collection of these data is necessary, patients must be informed that they could potentially be identified and must consent to this. Confidentiality clauses usually state that the individual will not be identifiable outside of the research team; wording may need to be changed in this scenario. • Invitation letters should be in the name of a healthcare professional involved in the patient's care. Similarly, a PIS should not be sent directly to a potential participant by a researcher outside of the clinical care team unless the patient has consented to be contacted. • Where consent is sought to use data/samples in future research, the PIS should contain enough information to allow informed consent. • Information should be provided on how long personal data will be kept. • Information on insurance (if included) should be consistent with the insurance arrangements. • References to the Data Protection Act should include the date 1998. • **Research involving children in England, Wales and Northern Ireland:** For CTIMPs, CT regulations apply: a minor is defined as someone under 16. Consent for children under 16 to participate in research must be given by a person with parental responsibility. In the rare circumstance that a person with

Check	Questions	Notes for completion
		parental responsibility is not available by reason of the emergency nature of the treatment, a legal representative would give consent. For non-CTIMPs, common law presumes that young people aged between 16 and 18 are usually competent to give consent to treatment and case law suggests if a young person is "Gillick competent" they can give consent to treatment. In the absence of law relating specifically to research for consent for non-CTIMPs, it is commonly assumed that the principle of "Gillick competence" can be applied to research. If participants are children (under 16) is consent being obtained from an adult? If there is no information on parental/adult consent for children, ask the researcher to confirm if (a) parental consent will be obtained and (b) assent will be recorded (assent refers to agreement by minors who have no legal right to consent – this is optional but may be recommended by a REC). • **NHS staff participants:** For staff studies, it is good practice to follow NRES guidance for PIS and consent forms. Check that these contain the key elements listed. Review how participants are identified to ensure it is appropriate and meets data protection. Use the above notes (for patient research) to inform completion of the check. • For studies originating in England (English Led, non CSP studies), does the PIS have a section which refers to PALS (Patient Advise and Liaison Service)?

Check	Questions	Notes for completion
		If YES, advise the researcher that: *"NHS Wales does not have a PALS and therefore the reference to PALS should be removed from the PIS to be used in Wales (i.e. on local documents submitted with SSI applications). Changes to remove a reference to PALS do not need to be submitted to REC as a substantial amendment."* If the researchers ask about an alternative in Wales, please note replacing the reference to PALS with a reference to anything other than "the NHS complaints procedure" may require REC review. • Personal data should not be transferred to another country outside the EEA unless the country ensures an adequate level of protection for the rights and freedom of data subjects in relation to processing of personal data. This should be detailed in the PIS and consent (check 2.1).
5.1	If personal data is being used is its use described in the PIS and will consent be obtained before personal data is collected?	The PIS should contain information on: • The purposes for which the data are to be processed • What data are to be collected • Who the information will be disclosed to • Whether any uses or disclosures are optional • Will publication include potentially identifiable personal data e.g. quotes? • Consent is not required when using anonymised data. Publication of quotes requires explanation in the PIS and specific consent on the consent form. Seek clarification if required e.g. how will direct quotes be appropriately anonymised.

Check	Questions	Notes for completion
5.1	Data confidentiality and security. ▪ How are data being moved between researchers/organisations (e.g. site to CRO)? ▪ What physical and electronic security measures are in place? ▪ What measures are in place to ensure confidentiality e.g. use of coded or anonymised data. Is the minimum necessary participant identifiable information being used? ▪ Who will have access to the personal data, what information will be accessed and is this covered by consent? ▪ Will researchers have access to full medical records and potentially sensitive health information? ▪ Physical transport of data (laptops, memory sticks, paper)?	Review protocol and IRAS form A36 – A45 CVUHB only permits emails with patient identifiable data to be sent between email addresses ending in …wales.nhs.uk. All patient identifiable data on laptops or portable media must be encrypted. ▪ All patient identifiable data on laptops or portable media must be encrypted. Things to look out for: • Personal data transferred electronically should be encrypted during transfer • Personal data should not be stored on home or personal computers • If it is necessary to use laptops and other portable devices, data must be encrypted and uploaded to secure server / desktop as soon as possible • Is the mechanism for data transfer between sites clearly described and secure • Confirm the destination of data from the site • For samples sent to CVUHB from other NHS organisations, CVUHB is the Data Processor and the site that the sample originated from is the Data Controller. Samples cannot be anonymised without the Data Controller first giving permission to do so. • Retrospective research on existing, non-sensitive data is acceptable, but only anonymised data may be used.

Check	Questions	Notes for completion
		• It should be noted that an assurance of maintaining confidentiality by someone receiving identifiable data does not provide a basis for access unless the access is given with consent or another legal basis.
5.1	What are the storage arrangements for personal data and research data?	• Review IRAS form A43 -45. • Sometimes the questions are incorrectly answered on the R&D form, as the researcher misunderstands the difference between personal and research data. Clarification may therefore be needed.
5.1	Will data be transferred to a country or territory outside the European Economic Area (EEA)?	• Personal data should not be transferred to another country outside the EEA unless the country ensures an adequate level of protection for the rights and freedom of data subjects in relation to processing of personal data. This should be detailed in the PIS and consent (check 2.1).

C2	Have any legal implications in the consent process been highlighted and addressed?	• Participants should normally receive information that is local to the site where they are participating in the study. Check that local information given to potential participants provides:
		  • Information about the site e.g. name of site, address and telephone number (usually included in the letterhead of the site)
		  • Contact details of the local investigator(s), and if applicable, other members of the research team, e.g. research nurses
		  • Emergency contact information, if appropriate

Check	Questions	Notes for completion
		• Contact information for complaints and, where appropriate, independent advisors See also Q2.1 notes for completion regarding requirements to ensure properly informed consent.
C16	Is access to personal identifiable information, for which this NHS organisation is responsible, in accordance with the organisation's policies? Are the individuals accessing the data allowed to do so? Do they have the necessary contracts/HRC/LoA?	• Where research is being undertaken through independent contractors, it is the independent contractor's responsibility to ensure that arrangements meet local policies and standards. Independent contractors may seek advice to meet their responsibilities.
C16	Are appropriate arrangements in place for secure access to, and processing of, personal identifiable information in accordance with the organisation's policies?	• This needs to comply with DPA principles relating to security of information. Need to know where information is stored what the security arrangements are and who will be able to access to ensure comply with DPA principle 7. which states that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In practice, it means there must be appropriate security to prevent the personal data held being accidentally or deliberately compromised. In particular, the research team needs to: • design and organise security to fit the nature of the personal data held and the harm that may result from a security breach;

Check	Questions	Notes for completion
		• be clear about who in the organisation is responsible for ensuring information security; • make sure there is the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and • be ready to respond to any breach of security swiftly and effectively. •
	Can arrangements for anonymisation or pseudonymisation of personal identifiable information set out in the protocol be undertaken locally, if relevant?	• This is usually detailed within the application documentation.
	Are arrangements for transfer of data to other organisations in accordance with the organisation's policies. Have arrangements been agreed between the relevant parties, e.g. in a Data Transfer Agreement?	• Liaise with the R&D contracts team to establish whether a Data Transfer Agreement is required.
	Can arrangements for storage and archiving of data at the site during and after the study be undertaken locally and are they compliant with local policy?	• The research should comply with R&D SOP, Archiving of clinical trial and research study data. Reference Number, UHB121, R&D ref number, SR-RG-001

3. RESOURCES

The guidance in section 2 below has largely been taken from the following sources:

- **NISCHR Permissions Coordinating Process Operating Guidelines**, v3.0 (consultation in use), 20 October 2014
- **NISCHR PCU Internal Guidelines for undertaking Study-Wide Governance Review (Interpreting UK Study-Wide Governance Checks)**, v2.0 (consultation in use), 6 may 2015

In addition, the following resources are available:

- **Information Security Management:**
  England, Wales and Northern Ireland: NHS Code of Practice:
  http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf

- **Records Management:**
  England, Wales and Northern Ireland NHS Code of Practice:
  http://systems.hscic.gov.uk/infogov/links/recordscop1.pdf and
  England, Wales and Northern Ireland:
  http://systems.hscic.gov.uk/infogov/links/recordscop2.pdf

- **NHS Information Governance – Guidance on Legal and Professional Obligations**
  England, Wales and Northern Ireland:
  http://systems.hscic.gov.uk/infogov/codes/lglobligat.pdf

- **England & Wales: Section 251 of NHS Act 2006 approval for the use of data without consent through the HRA Confidentiality Advisory Group** http://www.hra.nhs.uk/resources/confidentiality-advisory-group/

- **PIS/Consent guidance**
  http://www.hra.nhs.uk/resources/before-you-apply/consent-and-participation/consent-and-participant-information/

- **Confidentiality: NHS Code of Practice:**
  England: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
  A guide to confidentiality in health and social care
  http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf
  A guide to confidentiality in health and social care references
  http://www.hscic.gov.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf

- **Data Protection Guidance for Researchers**
  CVUHB document, version 1 - under consultation. Refer to CVUHB intranet for latest version.
- **Good Practice in Research and Consent to Research.** General Medical Council. March 2013, http://www.gmc-uk.org/Good_practice_in_research_and_consent_to_research.pdf_58834843.pdf

- **Information Commissioner's Office**
  'Guide to data protection'. https://ico.org.uk/for-organisations/guide-to-data-protection/