Public Benefit and Privacy Panel for Health and Social Care

Constitution and Terms of Reference

Abbreviations and Glossary

CHI number	Community Health Index number, used as the patient's NHS number in Scotland, and deemed to be an identifier in itself
CHIAG	CHI Advisory Group
DPIA	Data Protection Impact Assessment, an assessment of the privacy risks presented by different types of data processing. This is usually considered good practice; in some circumstances it is a legal requirement.
eDRIS	electronic Data and Innovation Service, as part of PHS, who provision data to applicants, support applicants for gaining the appropriate permissions and provide access to the National Safe Haven
GDPR	General Data Protection Regulation, incorporated into the UK Data Protection Act 2018.
HSC-PBPP	Public Benefit and Privacy Panel for Health and Social Care
ICO	Information Commissioner's Office, the body responsible for ensuring organisations comply with Data Protection Legislation
IG	Information Governance
IT	Information technology
NDS	NES Digital Service (involved in setting up the national digital platform, a central platform for public sector data in Scotland)
NES	NHS Education Scotland
NHSCR	NHS Central Register
NHS NSS	NHS National Services Scotland
NHSS	NHSScotland
NRS	National Records of Scotland
PAC	Privacy Advisory Committee (predecessor to HSC-PBPP)
PHS	Public Health Scotland
Tier 2 OOC	Tier 2 Out of Committee, a subgroup of the Tier 2 full committee, convened to review applications referred from the Tier 1 panel.

Constitution and Terms of Reference

1. The Public Benefit and Privacy Panel for Health and Social Care (HSC-PBPP) is a governance structure of NHSScotland (NHSS). It was established with delegated authority from NHSS Chief Executive Officers and the Registrar General of National Records of Scotland (NRS), for the NHS Central Register (NHSCR). Its remit is to carry out information governance (IG) scrutiny of requests for access to health data for purposes of health and social care administration, research and other well-defined and *bona fide* purposes, on behalf of individual data controllers[1]. The HSC-PBPP acts as the final arbiter of requests which fall within its remit, but does not replace any existing or future requirements for ethical review or approval. The HSC-PBPP has 'dotted line' reporting to Scottish Government eHealth.

2. The HSC-PBPP has a formal mandate to scrutinise requests to use NHSS-controlled data, and the NHSCR, controlled by the Registrar General, for research, healthcare planning, audit, or other well-defined and *bona fide* purposes. Its principal focus is on what are deemed national data-sets, data from more than one NHS Board, or cases involving data from one NHS Board which are highly complex, contentious or have national implications. Its remit relates to data which carry a risk of identifying individuals whether living or dead, and to creation of new linkages whether consent has been obtained or not. Access to clinical records for clinical research, with the consent of patients will not routinely be scrutinised by the HSC-PBPP, as this is usually covered by other governance processes. The HSC-PBPP is able, subject to capacity and the agreement of Data Controllers in other organisations, to scrutinise requests for use of health and social care data that is not controlled by NHS Scotland Boards (e.g. from local authorities, health and social care partnerships, GPs, etc.). Its full scope is included at Annex A.

3. The HSC-PBPP succeeds two previously existing processes in their scrutiny of applications for access to NHS-controlled data: NHS National Services Scotland's Privacy Advisory Committee (PAC) and the National Caldicott Scrutiny Panel. In addition, HSC-PBPP takes over responsibility from the CHI Advisory group (CHIAG) for scrutinising applications to use the Community Health Index (CHI) number and / or to access the CHI database for any purposes

[1] The delegation of information governance scrutiny of requests to access NHS Scotland-originated information, by NHS Scotland Chief Executive Officers and the Registrar General to the HSC-PBPP, in no way alters the obligations of these individual data controllers under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

other than NHS business and operational use, and especially for research or for commercial interest.

The HSC-PBPP does not replace any other existing local approval or scrutiny processes in operation within individual NHSS Boards (where local scrutiny is conducted for access to data owned by the individual board). It provides a single, simplified and truly national process, and prevents the creation of any further authority to deal with specific requests for access to data relating to more than one NHSS Board.

4. CHIAG will continue to scrutinise applications for NHS business and operational uses of the CHI number and the CHI database to support the delivery of health and social care.

5. The HSC-PBPP has a further mandate to establish and operate as a centre of excellence for privacy, confidentiality, and information governance expertise in relation to Health and Social Care in Scotland, providing strategic leadership and direction in this area to NHSS Boards, the research community, and wider stakeholder groups. In doing so it ensures connectivity between the many strands of relevant governance activity, and reacts to the changing landscape and research evidence regarding the public interest. The panel's focus on public awareness, concern and benefit demonstrates a commitment to the protection and promotion of privacy as a public good and in the public interest.

6. The HSC-PBPP operates to fulfil three main aims:
   - To provide a single, consistent, open and transparent scrutiny process allowing health and social care data to be used for a range of purposes including research.
   - To ensure the right balance is struck between safeguarding the privacy of all people in Scotland and the fiduciary duty of Scottish public bodies to make the best possible use of the health and social care data collected.
   - To provide leadership across a range of complex privacy and information governance issues, so that the people of Scotland are able to gain the benefits of better health and social care, from research and wider use of data, while managing emerging information risks, addressing public concerns around privacy, and promoting the protection of privacy as in the public interest.

7. The panel is supported by two HSC-PBPP managers and an administrator who are employed by Public Health Scotland (PHS).

HSC-PBPP Structure

8. The HSC-PBPP operates on a two-tier structure utilising a proportionate governance method, thus ensuring that scrutiny is proportionate, and that available resources are effectively used. Each of the two tiers focuses on the assessment of risk and the balancing of privacy risk with likely public benefit: the more operational Tier 1, guided largely by agreed proportionate governance criteria, and the more strategic Tier 2, guided by these criteria and the panel's guiding principles. The tiered structure provides for proportionality in the approval, conditional approval or refusal of applications to use data.

9. **Tier 1** assesses the more technical, security and legal aspects of requests for data, using agreed governance risk criteria and trigger points (included at Annex B) to determine whether access to data can be approved, or whether further scrutiny is required by Tier 2 colleagues. Tier 1 also advises applicants where evidence is insufficient or where proposed controls do not meet appropriate minimum standards.

10. **Tier 2** provides the intellectual space for senior leaders, Caldicott Guardians, researchers and public representatives to consider the wider privacy issues in regard to particularly contentious cases or proposed policies in NHS Scotland or the Scottish Government relating to the use of health and social care data. The work of Tier 2 comprises both a larger full committee, regularly convened, and a smaller group working 'out of committee' (Tier 2 OOC), convened as required to consider applications escalated or referred from Tier 1.

Panel Membership and Composition

11. Panel membership is as follows:

Tier 1

- Two Information Governance (IG) leads or practitioners from NHSS Boards (other than NHS National Services Scotland [NHS NSS] or PHS) and wherever possible, at least one from a territorial board. A rota for attendance by the NHS Board IG leads is drawn up by the HSC-PBPP administrator.
- One Information Governance practitioner from NHS NSS or PHS; a separate NSS / PHS rota is used to ensure that one of their IG leads will attend each tier 1 panel.
- Panel Manager (permanent member).

Quorum: 3 panel members, including 2 NHSS Board IG practitioners, and the panel manager.

- In the event that none of tier 1 has expertise in information technology (IT) security, separate advice from an IT Security Officer will be sought where deemed necessary, when data are to be accessed from outside an accredited safe haven.

Tier 2 (Full Committee)

- Chair (senior representative from an NHSS Board)
- Four public representatives
- Two representatives from the research community
- Three Caldicott Guardians from NHSS Boards, other than PHS or NHS NSS. In the event that a Caldicott Guardian cannot be available to sit on the committee, they should nominate a senior clinician from within their Board as their delegated representative.
- Caldicott Guardian for PHS or their delegated representative
- Senior representatives of each of the national data asset holders:
  - Senior representative of NHS NSS and CHIAG
  - Senior representative of NES Digital Services (NDS)
  - Senior representative of NRS
- Data linkage specialist (currently head of eDRIS)
- Senior representative from the National Records of Scotland
- Scottish Government IG Policy Lead;
- Senior social care representative.

Quorum: Chair + seven panel members, including the PHS Caldicott Guardian or their delegated representative, three other NHSS members and two public representatives
The panel managers and administrator attend the meeting for secretariat and information purposes.

Tier 2 (Out of Committee)

- Four public representatives;
- Three Caldicott Guardians or their delegated representatives from NHSS Boards other than NHS NSS or PHS;
- Caldicott Guardian for PHS or their delegated representative;
- Two research representatives

Quorum: Responses from five panel members, including two public representatives, two Caldicott Guardians from NHSS Boards and the PHS Caldicott Guardian or their delegated representative and/or one research representative (if responses from only two Caldicott Guardians are available).

Caldicott Guardians from NHSS Boards, who are not members of the committee may be co-opted to assess individual applications where any two of the three members of the committee are unable to do so. The panel manager will accommodate for this when quorum cannot be achieved.

12. The panel Chair is nominated and appointed by the Chief Executive Officers of the NHSS boards. Tier 2 committee members are appointed by the panel Chair, in the first instance following recommendations from Tier 2 committee or Operational group members. The panel's operational Tier 1 uses existing resources from within each NHSS Board.

13. The selection of panel members is based on the person specifications contained in Annex C.

14. Tier 2 committee members (including the Chair) may serve for an initial period of 3 years, renewable once. Ensuring adequate membership, for each of the panel's tiers, is the responsibility of the HSC-PBPP Chair. If required, those leaving the committee at the end of their second term can remain on the committee for a short time (e.g. six-months) to ensure smooth overlap with incoming new members, at the discretion of the panel Chair and agreement of the outgoing member. In the event of no suitable long-term candidates being found to replace those leaving the committee, after their second term, the HSC-PBPP Chair can co-opt these people back on to the committee on a short-term basis to ensure that the committee has quorum and can continue to function appropriately and efficiently.

15. Tier 2 committee members may resign at any point by informing the HSC-PBPP Chair in writing. The Chair may ask any panel member to resign at any time by writing to them, giving the reasons for the request.

16. Each Tier 2 committee member should endeavour to attend each committee meeting in person, or via tele- or video-conferencing. In the event that a committee member cannot attend a meeting, that they send in appropriate updates or comments regarding agenda items that they wish to be noted. However, Tier 2 committee members should not have deputies. If

a member fails to attend three consecutive meetings, without adequate reason, he/she will be deemed to have resigned. Where the role of Caldicott Guardian in an NHS Board is shared between two people, either person can take that position as member of the panel. In specific circumstances, Committee members can nominate an alternative person to attend the committee meeting, in place of a committee member. This could be, e.g., if the committee member knows they will be temporarily unavailable for committee meetings over a period of time. This would be subject to the following conditions:

- That the alternative person is not junior or deputy to the committee member; however, they could be someone more senior or of equivalent standing and expertise; e.g. a committee member in the Caldicott Guardian role, could nominate another Caldicott Guardian from another NHS Board, or assistant Medical Director.
- That the alternative person is suitably briefed on the agenda items for the meeting, by the committee member they wish to replace;
- That the alternative person is agreed by the Chair of the meeting.
- It is not recommended that lay people could be replaced by alternative persons, unless they are fully and specifically briefed regarding the issues involved.

17. The panel managers support the Chair in the operation of all aspects of the panel. The panel manager is a quorum member of the panel's operational Tier 1, but has no further decision-making responsibilities within Tier 2.

18. All panel members, from both tiers, must participate in appropriate training, agreed by the panel, in order to fulfil their role throughout their term of office.

19. Members are entitled to be reimbursed for travelling expenses.

20. The HSC-PBPP Operational Group was set up by the Tier 2 full committee to:
    - Identify and resolve issues that may affect the smooth running of the HSC-PBPP in order to protect the interests of all NHS Boards.
    - Provide support for the HSC-PBPP managers and administrative support staff.
    - Oversee the development & delivery of a HSC-PBPP work plan.

    Membership of this group consists of:
    - Tier 2 representative (Chair), currently PHS Caldicott Guardian or their delegated representative

- NHS NSS Data Protection officer
- Two NHSS IG Leads as representatives from Tier 1
- NHSCR representative
- eDRIS representative
- Panel Managers

There is no specific quorum for this group. The panel administrator attends this group for secretariat purposes.

Declarations and Conflicts of Interest

21. Committee members must inform the Chair if they have a financial, professional or personal interest in a project or with a project sponsor. For applications that have been referred for review by the full committee, the panel manager will inform the committee members of these referred applications, before the committee meeting papers are distributed. Any committee member who thinks they may have a conflict of interest for any of these applications must discuss it with the Chair at the earliest opportunity. **The Chair will decide whether the potential interest disqualifies the member from the discussion.** Unless a committee member is directly involved with the application (e.g. is the applicant / lead clinician / data custodian), or has an ongoing or recent (within the last two years) direct collaborative interest with the application or applicant, they should be able to remain in the meeting having declared their conflict of interest. The panel manager will maintain a Register of Members' Interest, which will be updated annually by members.

Panel Meetings and Process

22. PHS employs a team to provide data and support for applicants to HSC-PBPP: the electronic Data Research and Innovation Service (eDRIS). This team provides a single point of contact (eDRIS coordinator) for applicants for use of and access to data in a secure environment, assists applicants in their proposal design and supports applicants in as they complete the HSC-PBPP application form, and facilitates access to data in a secure environment. Members of the service team liaise with applicants and the HSC-PBPP managers to ensure that their application is valid and complete, before it is submitted for consideration by a Tier 1 panel.

23. The Tier 1 panels meet fortnightly and the Tier 2 full committee meets five times per year. Applications to the panel requiring Tier 2 OOC review, are considered by this group as required, and convened by the panel manager on behalf of the panel Chair. The Operational group meets as required, but usually soon (5-10 days) after a Tier 2 full committee meeting.

24. Applications submitted to HSC-PBPP will be sent to the next available Tier 1 panel, in accordance with submission deadlines, set and published by the panel manager. Such deadlines will allow Tier 1 panel members appropriate time to prepare for Tier 1 panel meetings.

25. Tier 1 panel meetings take place fortnightly to consider new applications, which must be submitted by the applicant prior to published application deadlines. A Tier 1 panel member rota is drawn up on a six-monthly basis by the panel administrator. Tier 1 members conduct independent assessments of each application prior to the panel meeting, using agreed proportionate governance criteria. The panel meeting is used to undertake group review of these assessments, using the same criteria to agree an outcome for the application: approved (with or without conditions), clarifications, resubmission, or referred to Tier 2. All panel members must agree for approval to be issued: failure to agree will result in referral or clarification (see below). For approved applications, the panel manager issues the agreed communication to the applicant, concluding the application process. For referred applications, the panel manager proceeds as outlined below.

26. Where a Tier 1 panel determines neither to approve nor refer an application, it may seek timely clarification or additional information from the applicant, in whatever form it deems necessary, in order to support its deliberations. This is facilitated by the panel manager, with a view to the Tier 1 panel members agreeing an outcome for the application (or alternatively the application returning to a subsequent Tier 1 panel), upon receipt of the necessary clarification or additional information. A Tier 1 panel will only seek clarification on an application which has a realistic chance of receiving approval upon receipt of the necessary clarification or additional information. Where an application clearly has little or no chance of approval, usually on the basis of a large amount of incomplete information, the panel manager will advise the applicant of this on behalf of the Tier 1 panel, with a recommendation to re-submit the application. Clarification may also be sought from the applicant in support of an application which is referred to Tier 2.

27. Monthly reports of the outcomes of application reviews and learning will be circulated around tier 1 panel members and relevant stakeholders (e.g. Caldicott Guardians). A performance report and application metrics will be presented to the Tier 2 full Committee at each meeting.

28. The Tier 2 OOC group, operating 'out of committee' (i.e. without meeting) is convened as required by the panel manager on behalf of the Chair, to review applications referred or escalated from Tier 1. The group is issued with the application to be reviewed, and the evidence of the deliberations of the Tier 1 panel. Members conduct independent review of the application and evidence, taking account of the agreed proportionate governance criteria, the panel's guiding principles, and other relevant considerations. They report their conclusions, independently, to the panel manager within the agreed timescale: that the application can be approved (with or without conditions), referred to the Tier 2 full committee, or cannot be approved. On receipt of clear approval from a quorum, and where no objections are expressed, within the agreed timescale, the panel manager issues the agreed communication to the applicant, concluding the application process. On receipt of an indication from a quorum that approval cannot be given, and where no approvals are indicated within the agreed timescale, the panel manager issues the agreed communication to the applicant, concluding the application process. In the case of any other outcome, the panel manager will establish whether further clarification from the applicant is likely to result in a decision being reached. Where this is not the case and strong objections remain, the panel manager will prepare the application for submission to the full committee, and will write to the applicant informing them of this.

29. The Tier 2 full committee is convened 5 times per year by the panel Chair. Each agenda includes relevant business items, regular items including review of applications from the last quarter, and any applications referred from Tier 2 colleagues out of committee. The committee agenda always places referred applications and review of recent applications before other relevant business items not associated with the application process.

30. The Tier 2 full committee considers referred applications and reaches a decision: approved (with or without conditions) or not approved, and the decision of the committee is final. Following the decision and recording of the rationale for the committee's decision in the minutes of the meeting, the panel manager will write to the applicant on behalf of the Chair,

outlining the decision. In the case where the application is not approved, the Chair may also personally contact the applicant to make them aware of the committee's decision.

31. Applicants may be asked to attend the HSC-PBPP Tier 2 committee meeting at which their application is discussed. Applicants will be given the opportunity to submit additional supporting material for the committee members and should do so in advance of that particular committee meeting.

32. Agenda and papers for Tier 2 full committee meetings shall to be sent to members within agreed timescales prior to the meeting at which they will be discussed. Late agenda items may be submitted at the discretion of the panel Chair.

33. All application outcomes will be issued to applicants by the panel manager within an agreed timescale of the decision being reached.

34. Minutes shall be taken of all Tier 2 full committee meetings, and will be submitted for approval to the next committee. Approved minutes shall be published on the HSC-PBPP website.

35. The panel manager, on behalf of the panel Chair, maintains a register of approved applications, which is made available on the HSC-PBPP website.

Expected Performance (Applications)

36. The HSC-PBPP recognises the need for timely scrutiny of applications, and ensuring that this is being achieved is the responsibility of the panel Chair. The panel manager monitors the performance of the panel in processing applications and reports on performance to the Tier 2 full committee, as part of the Panel Manager's report.

37. The panel manager will log the key events in the application process by date, for each application. For the purpose of monitoring performance, the time elapsed whilst awaiting clarification or additional information from the applicant will not be included within the recorded turnaround time (see below) for the application (i.e. the 'clock' will deemed to have been 'paused' whilst the applicant is responding). The total time taken for an application, from submission to outcome decision, will also be recorded.

38. Applicants are informed of Tier 1 panel decisions to approve (with or without conditions) applications within an agreed timescale after the panel's decision. It is the normal expectation that such applications will be concluded within 20-30 working days of receipt of an administratively complete application. Where clarification is required, this will be longer.

39. Applicants are informed of Tier 2 out of committee decisions to approve (with or without conditions), or not approve, applications within an agreed timescale after the group's decision. It is the normal expectation that such applications will be concluded within 60-90 working days of receipt of an administratively complete application.

40. Applications referred to the Tier 2 full committee are normally expected to be concluded within a period of 3-4 months, with the expectation being that only a small minority of applications reach this stage.

Amendment of Constitution and Terms of Reference

41. The Constitution and Terms of Reference are reviewed annually and may be updated more frequently if this is necessary.

42. The proportionate governance risk criteria and guiding principles, which form the basis for the panel's scrutiny of applications to use data, are owned by the HSC-PBPP and reviewed annually (as a minimum).

ANNEX A: Scope of Public Benefit and Privacy Panel applications

The HSC-PBPP has the authority to scrutinise any request to use NHSS-controlled data, and the NHSCR data controlled by the Registrar General, for research, healthcare planning, audit, or other well-defined and *bona fide* purposes. Its full, current, scope is laid out for potential applicants below.

Administrative data (including patient and staff data) have been collected and stored for purposes other than direct individual patient care. Examples of administrative health data include the Scottish Morbidity Records and similar data held by PHS or NSS.

You <u>must</u> complete an application if your proposal requires any of the following in respect of NHSS-originated data which carry a risk of identifying an individual

Its remit relates to

- All uses of administrative data from the national datasets or from more than one NHS Scotland Board, which carry a risk of identification of an individual, whether living or dead, including but not confined to:
    - Access to administrative health data
    - Linkage of administrative health data except within PHS where Standard Operating Procedures are followed to assess and mitigate risk
    - Linkage of administrative health data to administrative data from other sectors
    - Linkage of administrative health data to primary data collected by researchers **with or without consent**.
    - Transfer of such data outside NHS Scotland
- Access **without consent** to data held in individual patients' clinical records to be used for research either linked or unlinked.

You <u>may</u> complete an application for:

- Any other use of NHSS-originated data which you consider to be complex, contentious, having wider national implications, or requiring the scrutiny of the panel (including use of data from a single NHSS board)
- Use of data originating from primary care providers, and from beyond NHSS, but with a relevant implication for the service (for example social care information use).

The following relevant factors do not remove the requirement to complete an application (and should be fully explained at the relevant point in the application form):

- Consent of data subjects, **except** where consent has been obtained for access to clinical records as part of a clinical study
- Whether data subjects are alive or deceased
- Purpose of the proposed work is audit, management, performance, research or other
- Statutory or regulatory requirement for the proposed work

ANNEX B: Panel Guiding Principles and Proportionate Governance Criteria

Principles that guide the HSC-PBPP

In addition to the data protection and Caldicott principles, the following principles guide and inform the deliberations of the HSC-PBPP when considering applications to use NHSS-originated data:

Privacy

1. The starting point for considering any application to use NHSS-originated data is to recognise that everyone has a right to respect for their privacy.

Public interest

2. Before approving access to data, the HSC-PBPP must be satisfied that the public interest will be furthered by the proposal at hand, that there is both a demonstrable social need for such processing and a reasonable likelihood that it will result in tangible benefits for society.

Appropriate science

3. If applicants wish to process data in ways that may increase risk to privacy, then they must demonstrate that their research is scientifically-sound and ethically robust. This may be evidenced, for example, by approvals from an ethics committee and/or a scientific peer-review committee.

Consent

4. There is a general expectation that, wherever practicable, individuals should be made aware of the need to process their data, and consent obtained. Consent obtained for taking part in clinical studies is usually obtained according to the UK Research Governance Framework. This is different from specific consent to process personal or special category data, as outlined under the Data Protection Act 2018 and GDPR. But it is recognised that in some circumstances it is not possible or appropriate to obtain consent. In such circumstances, a clear explanation and justification should be given.

Transparency

5. Processing of data should fit with patients' reasonable expectations, the framework for which is set within NHSS policy and guidance. This would include privacy notice information on websites, general leaflets on confidentiality (e.g. 'How the NHS handles your personal information', available from the NHS Inform website), as well as in consent forms relevant to the processing.

Pseudonymisation or Anonymisation

6. Pseudonymising or anonymising data before release can considerably help to reduce risk to privacy**. Pseudonymised data** are data from which an individual can no longer be easily or immediately identified because information such as name or date of birth, have been removed or masked, but the identifiers are still held, and linkage can still be made back to the original person. Such data are still classed as personal data under data protection legislation. **Anonymised data** are data from which an individual can no longer be identified because information such as name or date of birth, have been removed or masked, and that link is permanently broken, so that there is no way by which any individual can be re-identified. The HSC-PBPP operates on the basis that data should be anonymised as fully as possible, consistent with their use. However, sometimes it is not

appropriate to fully anonymise the data because this will interfere with legitimate processing. In such circumstances, a clear explanation and justification should be given.

Privacy impact

7. The HSC-PBPP must be satisfied that any impact on individual privacy is clearly outweighed by the public benefit resulting from the processing, and in any case is reduced to the absolute minimum necessary to achieve the outcomes of the proposal. Any likely impact on individual privacy should, therefore, be fully explained to allow a meaningful assessment of the risk.

Safeguards

8. If special safeguards are to be used to protect individual privacy, these must be described and meet acceptable standards.

Security

9. The HSC-PBPP must be satisfied that data will be held securely as long as they remain in the custody of the recipients.

Proportionality

10. Processing of data must be proportionate to the objectives. This can only be assessed on a case-by-case basis but it signals that processing should be no more than necessary to meet the social need. Relevant factors include the type and amount of information to be use or linked, and the nature and number of parties to whom it is to be disclosed. Use of data will be approved only for the purpose/s detailed in an application, and will not extend to any use for additional or secondary purposes.

Precedent

11. The HSC-PBPP will reflect on the precedents which its own past decision making, and the decision making of its antecedents (as far as these can be deemed to be relevant and in keeping with good practice and its own principles), represent, and will take these into account where they are relevant to the application at hand.

Proportionate Governance Criteria

Safe People	
Question 1 Is the applicant, data custodian, clinical lead, and everyone who will have contact with the identifiable or potentially identifiable data trained in Information Governance*? Are there any concerns regarding the suitability of any person in each of the main roles? *Approved training courses are listed in Appendix A of the Applicant Guidance Notes	
Roles	**Application coordinator** to ensure this information is provided on form
Key Question	**No** but no approval will be given without evidence that relevant training is completed. An amber response requires further work to establish if applicants are adequately trained.
Relevant questions	**Questions 1.1 – 1.5**
Green	Yes, has completed or will undertake approved training or verifiable appropriate training
Amber	Reports training but difficult to assess, or only some participants trained
Red	Unable to establish training status or efficacy of training

In assessing the Information Governance training undertaken by individuals who will have contact with the data, and whether this is acceptable, colleagues may consider:

- Which roles within the proposal each individual is undertaking, and whether the level or detail of training undertaken is commensurate with their responsibilities in respect of data.
- Whether the training specified is included on the list of approved/recognised training provided at table 4 of Appendix A below, or if not, what evidence supports its value in giving assurance to the panel.
- Any evidence provided which confirms that training has been undertaken.

Safe Organisations	
Question 2 Are all organisations engaged in the proposal verifiable as *bona fide*? Is the main contact for the lead organisation suitable to ensure organisational accountability for the data, and not filled by anyone also in section 1?	
Roles	**Tier 1 panel** will assess
Key Question	**No**
Relevant questions	**Section 2**
Green	Known partner organisations, NHSS boards, NHS trusts, UK public bodies, UK academic organisations, other recognisable UK organisations, which are registered with the ICO as a data controller
Amber	Yes, based outside UK
Red	No

In assessing each of the organisations engaged in the proposal, and whether these can reasonably be considered as bona fide, colleagues may consider:

- Whether the organisation belongs to the groups mentioned above (known partner organisations, NHSS boards, NHS trusts, UK public bodies, UK academic organisations, other recognisable UK organisations, which are registered with the Information Commissioner's Office (ICO) as a data controller.
- Whether the organisation is otherwise registered with the ICO as a data controller.
- Whether the organisation is registered with the Office of the Scottish Charities Regulator.
- Whether the organisation has an existing contractual relationship with one or more NHSS boards.
- Any evidence of governance or reporting arrangements in relation to the organisation which might indicate accountability to an organisation of the type listed above (particularly relevant for collaborative networks, for example).

Public Interest	
Question 3 Has the applicant demonstrated how their proposal will benefit patients or public?	
Roles	**Tier 1 panel** to assess whether reasonable case is made for necessity or benefit of proposal, or whether statutory duty exists
Key Question	**Yes,** if red, refer
Relevant questions	**Specifically Q 3.1.08 (but see also Q 3.1.06–3.1.11 and Q 5.4.01a [dissemination of results])**
Green	Yes, or statutory duty exists
Amber	Insufficient consideration given to issue or difficult to establish
Red	No evidence benefit patients or public

In assessing the benefit to patients or public which will result from the proposal, colleagues may consider:

- Whether a clear chain of cause and effect between the processing of data and the resulting demonstrable benefit to patients or public has been clearly and convincingly articulated in the proposal.
- Previous proposals reviewed by the panel which share similarities in terms of benefit to patients or public to this proposal, and the outcomes of these (i.e. precedent within the panel).
- Whether the proposal is responding to a statutory or regulatory requirement upon the applicant or sponsoring organisation.
- The likelihood and level of assurance given that benefit will be forthcoming.
- The Scottish Government's Guiding Principles for Data linkage (2012).

Safe Project	
Question 4 Is the proposal design and method appropriate to its objectives? Are the data and variables requested justified, appropriate, necessary and sufficient for the objectives and questions being addressed?	
Roles	Where appropriate, the **eDRIS coordinator** will work with applicant prior to submission to ensure that proposal design and methods of using data, and the data variables requested, are sufficient and appropriate to its objectives. **Tier 1 panel** will assess, taking into account any concerns reported by the eDRIS coordinator, whether proposed use of data and method of processing is appropriate; clarity of understanding is important.
Key Question	**Yes,** if proposal preparation well advanced and redesign not possible, refer
Relevant questions	**Q 3.1.09–3.1.11** (project description) and **Q 4.1–4.5** (variables)
Green	Yes
Amber	Doubts, queries or issues with proposed design or method, given objectives. Proposed processing goes beyond that required to achieve objectives
Red	Unlikely the objectives will be met

In assessing the appropriateness of the design and method to the objectives of the proposal, colleagues may consider:

- The clarity with which the design, method and objectives have been articulated.
- The common law Duty of Confidentiality.
- The Data Protection Act / GDPR 2018 and its principles.
- The Caldicott Principles, in particular principles 1 (Justify the Purpose), 2 (Don't use patient identifiable information unless it is necessary), 3 (Use the minimum necessary patient identifiable information), and 4 (Access to patient identifiable information should be on a strict need-to-know basis).
- NHSS Code of Practice on Protecting Patient Confidentiality (2012).
- The Scottish Government's Guiding Principles for Data linkage (2012).
- The Information Commissioner's Office guidance and codes of practice on anonymisation and data sharing and privacy by design.

Safe Data	
Question 5 Are the data highly sensitive or relating to vulnerable populations? Personal data regarding health are in a 'Special Data category' according to GDPR. The personal data are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and the context of their processing should be considered in respect of any significant risks to the fundamental rights and freedoms. Within the special category, there are data that could be thought of as highly sensitive data and particularly vulnerable populations and are listed below.	
Roles	**Tier 1 panel** to assess
Key Question	**No.**
Relevant questions	**Q 3.1.12, Q 3.1.13, Q 4.2 and Q 4.3.**
Green	No, no vulnerable populations or highly sensitive data will be included (this is quite rare). Health is the only special category data requested.
Amber	Some highly sensitive data will be used but this is not the focus of the proposal. Some highly sensitive data will be used and/or vulnerable populations involved, but controls appear adequate and commensurate with sensitivity/vulnerability. Focus of research may be considered sensitive although not on list. The application includes other special category data as well as health.
Red	Highly sensitive data or highly vulnerable populations are the focus of the proposal and/or there is insufficient evidence of adequate controls.

In assessing sensitivity of data, and the controls in place in respect of this, colleagues may consider:

- Vulnerable populations (not exhaustive): Adults with Incapacity, Drug users, homeless, those with mental health issues, Babies and children, minority ethnic groups, specific religious affiliation
- Highly sensitive data (not exhaustive): Sexual orientation and sex life (includes sexually transmitted diseases), mental and physical health data, Pregnancy in age < 16 years, Drugs and alcohol misuse, Religion, Suicide, Race / Ethnicity, Genetics, Biometrics.
- NHSS Code of Practice on Protecting Patient Confidentiality (2012).

Safe Project	
Question 6 Has appropriate peer review, lay consultation / public engagement and privacy risk assessment (DPIA) been undertaken?	
Roles	**Tier 1 panel** will assess whether each is appropriate or necessary
Key Question	**No,** but Tier 2 is keen that lay input is emphasised, especially for research.
Relevant questions	**Q 3.1.15–3.1.17 and any supporting documents.**
Green	Appropriate actions have been undertaken
Amber	Some appropriate actions which could reasonably and practically be expected have not been undertaken
Red	Peer review, lay consultation or privacy assessment is highly desirable or mandatory but has not been undertaken

In assessing the appropriateness of any peer review, lay consultation or privacy assessment undertaken, colleagues may consider the relevance of each in the context of the proposal and the assurance which each does, or would, demonstrate.

In addition, colleagues should consider:

- The value of external scientific peer review in providing additional assurance in respect of method, design and objectives of the proposal.
- The value of lay consultation in providing additional assurance in respect of public or patient benefit, and of indicating any potential public or patient concern which might arise from the proposal.
- Whether the public engagement programme is proportionate to the privacy risk of the application.
- The requirement of a Data Protection Impact Assessment (DPIA) in providing additional assurance that privacy risk has been adequately assessed, is appropriately managed, and can be reduced to acceptably low levels. Importantly in cases of high risk processing, under new data protection law a DPIA is a legal requirement and to proceed without one would therefore be unlawful.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Safe Projects	
Question 7 Is there any concern regarding commercial interest or involvement in the proposal?	
Roles	**Tier 1 panel** will assess
Key Question	**Yes, if assurances regarding commercial involvement not received, refer.**
Relevant questions	**Section 2** and **Q 3.1.18.**
Green	No commercial interest or involvement.
Amber	Commercial interest in the proposal as well as public health interest (e.g. active involvement of health technology provider or pharmaceutical company), but where public benefit clear and no privacy concerns.
Red	Clear commercial interest in, or motivation for, the proposal (e.g. commercially funded) considered to outweigh, or potentially outweigh, public interest, or presenting privacy concerns.

In assessing any commercial interest or involvement in the proposal, colleagues may consider:

- Any dependency between the benefit to patients and public likely to arise, and the commercial involvement or interest in the proposal.
- Any conflicts of interest arising or reasonably foreseeable as a result of commercial interest in the proposal.
- Any unintended, unforeseen or undisclosed commercial interest that might result from the proposal and conflict with or compromise the public interest, or present privacy concerns.
- Any commercial companies that might be contracted to process data on behalf of the applicants.

Lawful processing of data	
Question 8 Is the lawful basis for processing data for the proposal clear and appropriately evidenced?	
Roles	**eDRIS coordinator** to ensure this information is provided where non-NHSS data controllers are identified in section 4.1, 4.2 and 4.5. Under GDPR a legal basis for processing personal data is required under article 6 and a legal basis for processing special category data is required under article 9. **Tier 1 panel** to assess
Key Question	**Yes, if red, refer**
Relevant questions	**Q 2, Q 3.1.05, Q 3.2, Q 4.2 & Q 5.3.03.**
Green	Yes, Data protection legal bases for processing are required and have been satisfied. Data controller permission is in place for non-NHS Scotland data, and any data transfer beyond the UK is adequately controlled. Appropriate Data Processing / Sharing Agreements are in place (where required).
Amber	Some concerns remain:- the basis for legal processing may be unclear, data controller permissions or registrations are unclear, or other concerns remain
Red	Risk that proposal may result in unlawful processing is evident

In assessing the legal basis for the proposal, colleagues may consider:

- The common law Duty of Confidentiality.
- The first principle of Data Protection law (Personal data shall be processed fairly, lawfully and transparently), including the requirement for processing to be in line with relevant conditions from Articles 6 and 9 of GDPR.
- The Caldicott Principles, in particular principle 6 (Understand and comply with the law).
- Evidence of appropriate permission to process data from sources beyond NHS Scotland.
- Any statutory or regulatory requirement upon the applicant or sponsoring organisation.
- Any data to be placed in the National Safe Haven will be accessed by the applicant as pseudonymised data. The personal identifiers will have been processed by eDRIS /NRS.

Participant awareness	
Question 9 Are individuals aware of the use of their data or is the use wholly compatible with that for which the data was originally collected? Are the patient/public-facing information leaflets, patient information sheets, consent forms and website links sufficient, appropriate and available to the study population, and appropriate for the extent of the use of their data? **Note:** Data collected specifically for the purposes of research is likely to warrant a patient information leaflet and consent form. Data collected for the purpose of administering public services is likely to warrant a privacy notice or other evidence of fair processing.	
Roles	**Tier 1 panel** will assess
Key Question	**Yes, if red, refer**
Relevant questions	**Sections 4.2 and 4.3.**
Green	Populations of individuals involved are clearly informed or robust attempts to inform have been made (e.g. clear patient information and / or consent for purposes of the proposal and use of the data).
Amber	Limited evidence that individuals are aware that their data may be used in this way and limited attempts to inform, but with understandable practical difficulties to doing so. The purpose is in line with the original purpose of collection **and** is one they might reasonably expect
Red	No evidence that individuals are aware that their data may be used in this way and limited attempts to inform, where it is reasonably practical and possible do so. The purpose is **not** in line with the original purpose of collection and is **not** one they might reasonably expect.

In assessing awareness of data subjects and compatibility with the original purposes of data collection, colleagues may consider:

- The strength of evidence provided in respect of fair processing, patient or participant information, and/or consent.
- The time elapsed since the patient information leaflet and consent forms were produced / used
- The common law Duty of Confidentiality.
- The first principle of the Data Protection Act (Personal data shall be processed fairly, lawfully and transparently).

- Any issues which might challenge the validity of consent or the capacity of individuals to provide consent.
- Any issues which might challenge the practicality of obtaining consent or informing patients.

Safe Project	
Question 10 Does the proposal require any direct contact with groups of individuals, whether patients/public or other relevant groups (e.g. clinicians, family members, control sample), either by the applicant directly or by proxy through an NHSS board, GP, or other third party (on the applicant's behalf)?	
Roles	**Tier 1 panel** to assess
Key Question	**Yes, if red, refer.**
Relevant questions	**Q 4.6**
Green	No
Amber	Yes, contacting individuals who have consented to be contacted for the purposes outlined in the proposal. In some cases, contacting individuals who may not have consented to be contacted (e.g. NHS Scotland employees). Yes, contacting individuals who have not consented to be contacted, but initial contact is through a GP or a clinician or NHS service known to the patient.
Red	Yes, contacting individuals who have not consented to be contacted for the purposes outlined in the proposal, or have not consented to be contacted at all.

In assessing any direct contact with individuals, colleagues may consider:

- The common law Duty of Confidentiality.
- The first principle of the data protection law (Personal data shall be processed fairly, lawfully and transparently)
- Current NHSS and research best practice recommendations on making contact with patients and public.
- NHS Scotland Code of Practice on Protecting Patient Confidentiality (2012).

Safe Projects	
Question 11 Is risk of unintended disclosure minimised, with appropriate controls applied?	
Roles	**Tier 1 panel to c**onsider the combination of variables, risk arising from access to individual identifiable data, and risk of re-identification or unintended disclosure; consider controls alongside data and variables Where appropriate, **eDRIS coordinators** can confirm that detail is essential to meet objectives
Key Question	**Yes, if red, refer**
Relevant questions	**Q 3.4, Q 4.3 and Section 5**.
Green	Yes, no outstanding concerns regarding unintended disclosure
Amber	Some residual risk remains giving concern. Residual risk difficult to assess or assessment based on highly unpredictable factors. Very low risk competing with very serious potential consequences. Appropriate controls not in place or merely pending
Red	Residual risk to individual identifiable data remains unacceptably high given likely benefit. Harm or potential harm to individuals is reasonably foreseeable. Residual risk has the potential to be reasonably reduced further.

In assessing risks of unintended disclosure, colleagues may consider:

- The common law Duty of Confidentiality.
- Data Protection law and its principles.
- The Caldicott Principles, in particular principles 1 (Justify the Purpose), 2 (Don't use patient identifiable information unless it is necessary), 3 (Use the minimum necessary patient identifiable information), and 4 (Access to patient identifiable information should be on a strict need-to-know basis).
- NHS Scotland Code of Practice on Protecting Patient Confidentiality (2012).
- The Scottish Government's Guiding Principles for Data linkage (2012).
- The Information Commissioner's Office guidance and codes of practice on anonymisation and data sharing and privacy by design.
- Use of a recognised Safe Haven.

Safe Environment and Outputs	
Question 12 Are information security controls adequate? To provide additional assurance where explicitly technical risk is evident	
Roles	**Panel Security Advisors** to be consulted by **Tier 1 panel** where appropriate
Key Question	**No**
Relevant questions	**Q 3.4 and Section 5.**
Green	Data will be accessed exclusively through an accredited safe haven, or there is no residual risk resulting from lack of technical controls, outstanding technical vulnerability, or reasonably foreseeable technical threat
Amber	Data will be processed using technology which might expose it to reasonably foreseeable technical threat or where there is outstanding technical vulnerability or lack of controls giving some concern
Red	Outstanding concerns regarding technical threat, vulnerability or control which cannot be satisfactorily addressed

In assessing information security controls in place, colleagues may consider:

- Current NHSS best practice in Information Security and Information Security Management Systems, available through a series of good practice guides.

General	
Question 13 Does the application pose any privacy or ethical concerns not addressed above?	
Roles	**Tier 1 panel** to assess
Key Question	**Yes, if red, refer**
Relevant questions	**All sections and questions**
Green	No
Amber	Yes, mild to moderately serious concern remains. Please describe the concern.
Red	Yes, there is serious concern. Please describe the concern.

Additional or remaining ethical, privacy or other concerns arising from the proposal should be captured for discussion at the Tier 1 panel meeting.

ANNEX C: HSC-PBPP Role and Member Specifications

1. Tier 2 (strategic) committee member

The **role** of committee members is to:

- Review applications for use of NHSS and other personal or sensitive data, as outlined in the panel terms of reference
- Review applications in light of the panel's own proportionate governance criteria, guiding principles, and other instruments concerning privacy protection and information risk management
- Bringing to bear their relevant experience, indicate as required their opinions or decisions in respect of such applications, and in respect of other relevant panel business

It is **essential** that those members:

- Exercise dispassionate and unbiased judgement regarding ethically and practically complex and finely-balanced issues
- Express the reasons for their decision making concretely and concisely
- Rapidly assimilate and understand large amounts of information about high-level medical and social project proposals
- Are familiar with the current legislative and advisory environment regarding personal data, especially health data
- Contribute to out of committee activities as requested, responding in a timely manner
- Are suitably equipped to participate fully in the work of the panel by electronic means
- Undertake any training as might be deemed appropriate by the panel Chair
- Attend five half-day meetings per year

It is **desirable** those members:

- Maintain a strong interest in a field relevant to the Panel's work, such as patient rights, privacy law or data protection, Caldicott, medical and / or research ethics, or medical or statistical research

2. Tier 1 (operational) panel participant

The **role** of a Tier 1 panel participant is to:

- Review applications for access to NHSS and other personal or sensitive data, as outlined in the panel terms of reference
- Review applications in light of the panel's own precedents, including its proportionate governance criteria, and other instruments concerning privacy protection
- Bringing to bear their relevant experience, indicating as required their opinions or decisions in respect of such applications

It is **essential** those members:

- Currently hold a dedicated Information Governance role within an NHSS Board (territorial or national) and are of a suitably qualified nature to fully participate in the decision making of the panel (the panel Chair will make any determination required)
- Exercise dispassionate and unbiased judgement regarding ethically and practically complex and finely-balanced issues
- Express the reasons for their decision making concretely and concisely
- Rapidly to assimilate and understand large amounts of information about high-level medical and social project proposals
- Are familiar with the current legislative and advisory environment regarding personal data, especially health data
- Contribute to panel activities as requested, responding in a timely manner
- Attend up to four one-day panel meetings per year, each of which will require approximately one day's preparatory work
- Are suitably equipped to participate fully in the work of the panel by electronic means
- Undertake any training as might be deemed appropriate by the panel Chair

It is **desirable** those participants:

- Have an excellent level of current knowledge of the relevant legislative and advisory landscape

3. HSC-PBPP Chair

The **role** of the panel Chair is to:

- Ensure that the panel operates within its terms of reference.
- Ensure that the panel meets any performance targets or obligations set out in its terms of reference.
- Ensure that the panel's Tiers are adequately resourced with suitably qualified members, liaising with NHSS Chief Executive Officers and other relevant stakeholders to achieve this.
- Ensure that any issues of competing interests among members are dealt with appropriately.
- Ensure that the panel is effective in its role as final arbiter of submitted applications, providing appropriate, proportionate and consistent scrutiny over time.
- Ensure that the panel's deliberations and discussions are informed by all relevant current legislation, guidelines and policies, as well as the panel's own precedents.
- Ensure that the panel's deliberations account for the interests and opinions of the wider public, and acts in its interests.
- Provide strong and effective leadership to the panel in fostering productive relationships with both the public and the applicant community.

It is **essential** that the Chair:

- Is currently a non-executive Director of an NHSS board
- Maintains a strong interest in a field relevant to the Panel's work, such as patient rights, privacy law or data protection, Caldicott, medical and/or research ethics, or medical or statistical research
- Is familiar with the current legislative and advisory environment regarding personal data, especially health data
- Displays strong leadership and influencing skills and can focus the deliberations of a diverse and well-qualified panel on constructive and clear decision making
- Exercises dispassionate and unbiased judgement regarding ethically and practically complex and finely-balanced issues
- Expresses the reasons for their decision making concretely and concisely
- Rapidly assimilates and understands large amounts of information about medical and social project proposals
- Attends five half-day meetings per year

It is **desirable** that the Chair:

- Has an excellent level of current knowledge of the relevant legislative and advisory landscape.
- Does not currently hold their NHSS board's central information governance function within their management portfolio.

4. Panel Managers

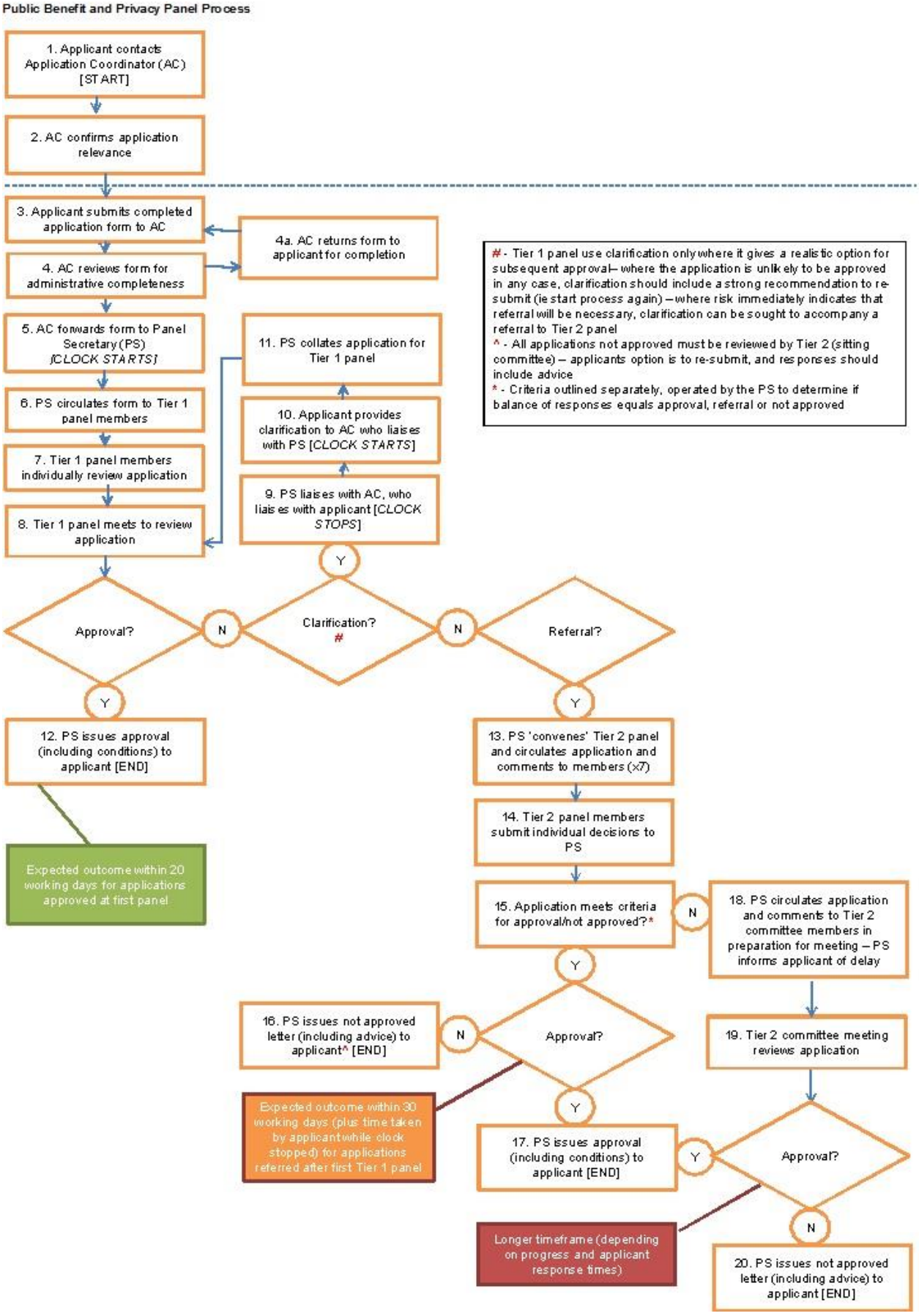
The **role** of the panel Manager is to:

- Assist the panel chair in ensuring that the panel operates within its terms of reference;
- Assist the panel chair in ensuring that the panel meets any performance targets or obligations set out in its terms of reference;
- Assist the panel chair in ensuring that the panel's Tiers are adequately resourced with suitably qualified members;
- Ensuring the smooth administrative operation of the panel's work;
- Assist the panel members in undertaking their responsibilities in an effective and timely manner;
- Participate in full in the work of panel's operational Tier 1.

It is **essential** that the Managers:

- Are familiar with the current legislative and advisory environment regarding personal data, especially health data
- Display excellent organisational and communications skills
- Undertake any training as might be deemed appropriate by the panel Chair

ANNEX D: Application Process Map



ANNEX E: Application Outcome Criteria

Tier 1

- Approval (with or without conditions): All members agree on approval (based on proportionate governance assessment); any approval conditions are specified by the members.
- Referral: One or more members request referral to Tier 2 OOC (based on proportionate governance assessment).
- Clarification: can be used for applications which Tier 1 members consider likely to gain approval, but requires some clarifications, minor changes and / or further information.
- Re-submission: can be used for applications which Tier 1 consider unlikely to gain approval in its current conditions, but with some major changes recommended by the panel members should be resubmitted,

Tier 2 Out of Committee

- Approval (with or without conditions): All members indicate approval to panel manager; any approval conditions are specified by the members.
- Referral: One or more members indicate to panel manager that the application cannot be approved, or that significant concerns remain and should be referred to the full Tier 2 committee.
- Clarification: can be used for applications which Tier 2 OOC members consider likely to gain approval, but requires some clarifications, minor changes and / or further information.
- Not Approved: All members indicate to panel manager that the application cannot be approved. This recommendation should always be provided with advice to applicant, including the option to re-apply, and all such outcomes must be reviewed by the Tier 2 full Committee.

Tier 2 Full Committee

- Approval: the Chair indicates to the panel manager that the application is approved
- Not Approved: the Chair indicates to panel manager that the application cannot be approved