Example Audit Plan

Projects need to plan for annual reviews of (including audits of effectiveness), including:

- Tier 1 and Tier 2 Information Sharing Agreements
- Privacy Impact Assessment
- Communications/Informing Strategy
- Security policies
- Privacy audits (checking appropriate use of systems and access controls)

Privacy Audit Activities

Where systems have the potential to override dissent or to enable access without consent through an override function, there will need to be a plan to audit any activity where an override occurred.

It is expected the vast majority of use and access will be appropriate. The functions exist both to record the basis/justification but also act as a deterrent to inappropriate use. The 'deterrent' aspect of the function should be reasonably effective, but will be more effective if users are subject to periodic checks. The following checks are proposed:

i. Consent/Legitimate relationship checks

A random sample of users should be checked to see the basis on which they are claiming consent or a relationship to the individual. This should be done across the spectrum of organisations contributing data to the portal. This can either be done by a central audit, that links to key staff in each organisation, or by a distributed function where key staff audit their own employees directly. For phase 1, initial processes will be centralised to identify cases to check, but these will then be passed to each stakeholder to identify corroborating evidence.

Sources of corroborating evidence: These will vary to a degree depending on the LR claimed, but will generally work on the basis of:

- Individual Consent LR – This can be corroborated with data on the user's source system. Where there is no corroboration this should be challenged with the user. As a last resort this could be corroborated directly with the individual, however this should be approached with caution.
- Referral to service LR – the main source system for the user's organisation should be able to confirm if service is provided to the individual. Or central records should confirm if the patient is registered with the general practice.
- Urgent Care LR – as above systems within the urgent care centre should have corroborating data.

ii. Legitimate reasons (privacy 'break the seal') checks

As most activity will be via LRs, there should be less privacy seal breaks to check. Again it is proposed that a sample are checked in a similar manner. It is also proposed that alerts on these are sent to identified 'privacy officers'.

Sources of corroborating evidence:

- System Admin – The Back Office function should be able to evidence the request/call received for assistance that links to the privacy seal break
- Care Quality (audit/investigation) – This may be where the user has accessed the data for these purposes at the request of another initiative, such as an investigation into alleged poor care. They may have had to provide data to another (investigating officer). Many of these (although few are expected) will be in response to a request, so the trail back to the request can be checked.
- Referral Check – This is to be used where there is doubt about accepting a referral, so no LR may be created. There should be evidence of the request for referral, even if it was rejected
- Safe Guarding concerns – The user should be able to provide detail of the concerns. There may be general concerns about the individual or a request to provide data into a safeguarding situation

Other audit activities:

Checks will need to be performed as follows:

Activity of a user – to be able to show what a user has done over a period of time, in case there is a need to support an investigation into a user's activity

Who has accessed an individual's record – to be able to show which users have accessed the individual's record. Potentially at the request of the individual or as part of an investigation/complaint made by the individual.