Ethics and Privacy Issues for Research and Evaluation

Ethics

Currently many research projects registered with the Research Office (RO) at Counties Manukau Health are out-of-scope for the Health and Disability Ethics Committee (HDEC) review process for ethics approval. Typically, out of scope audit, research or evaluation projects do not undergo any other form of formal ethics review and approval. This means that investigators frequently miss opportunities to improve the quality of their research and ethical conduct of their research practice, and also to improve their own working knowledge of ethics guidelines, requirements and practices. In some cases, projects may benefit from undergoing ethics review with another committee. This is particularly relevant where researchers want to:

- approach patients directly. This requires an informed consent process.
- interview or gather information on staff opinion or experience.
- obtain identifiable data about patients (e.g. gathering NHIs, or directly accessing whole patient notes) (also see the privacy section below)
- publish their research results. This requires planning for ethical requirements from the beginning, particularly as publishing in certain outlets have specific ethical criteria.

An existing guideline ‘Ethical Guidelines for Quality Improvement’ exists to support staff in thinking ethically about their projects. This guideline recognises that quality improvement (QI) and research activity are on a continuum of activities concerned with making changes and measuring their impacts with the aim of better understanding, or improving processes and/or outcomes. As with research and evaluation, QI may have unexpected adverse consequences, involve activities requiring patient consent, and contribute to knowledge which influences the ongoing provision of healthcare. It is therefore reasonable that QI projects should receive at least some consideration of ethical implications, undergo an approval process when appropriate, and be underpinned by the same ethical principles as those which apply to research and evaluation in healthcare.

The guideline and flow diagram are one of a few resources available to staff. Researchers can refer to the attached flow diagram which is intended as an education and support resource to help researchers to identify and resolve ethical and privacy issues in their work, and also direct in some clear instances, where ethics approval may be required.

1 http://cmdhbdocuments/docsdir/opendocument.aspx?id=A528791
Data Privacy

There are numerous risks to data privacy in relation to research and evaluation. Principles for good data storage include that:

- data is only accessible to the defined research or evaluation team
- appropriate security specifications are in place (e.g. some cloud providers may not have adequate security settings for the storage of data and so are not acceptable places to store data)
- patient consent for storage of data has been obtained
- data is properly anonymised
- health information is kept for the appropriate amount of time (see below) and then destroyed
- data is used only to answer the research question for which it was collected, not for other purposes

Health Information* is often used in research or evaluation, for example, to monitor patient health outcomes. The Privacy Code 1994 outlines key requirements regarding how Health Information that is collected from patients during the delivery of care at CM Health is used and managed. Key steps or responsibilities for keeping health information secure that staff should be aware of include that they should:

- Read "Health Research and Privacy: Guidance notes for health researchers and ethics committees**
- Sign a confidentiality agreement (available from research office) and upload it with the research application to the research office. This is relevant to any staff with access to the research data.
- Only transfer Health Information** by email to those within the regional secure network (any Middlemore, Waitemata or ADHB email) who are members of the research team.
- Encrypt or password-protect any data storage devices (e.g. USB flash drives) used to store health information.
- Password-protect any files containing Health Information.
- Keep any hardcopy Health Information that relates to identifiable individuals for 10 years and then destroy it in a secure bin.

**Note: anonymised information which cannot be linked to identifiable individuals is not regarded as Health Information by the Health Information Privacy Code (1994).