Introduction
With the advances of information technology in health institutions and the adoption of electronic medical records, questions emerge on how these changes affect patients’ rights regarding privacy and confidentiality. Expedient access to important information for medical treatment and research purposes are popular advantages to employing information technology in health organisations. Data used for unethical or commercial purposes can however compromise the adoption of this new technology. Therefore it is important to ensure that health services adopt the highest possible standards in their use of electronic patient data.
This review aims to:
1. Identify established legal and ethical standards for privacy and confidentiality issues relating to electronic governance, and
2. Establish best practice standards for those issues where ambiguity may exist in health service delivery.

Methods
1. A literature review to establish relevant principles of law and ethics relating to privacy and confidentiality in the health services. Examination of these in relation to local practices identified grey areas in the application of these laws.
2. Based on these findings, a survey instrument was prepared in order to obtain more information about current practices in relation to the grey areas identified
3. A convenient sample of 14 hospitals (Australian and international) which used advanced electronic patient systems, and were therefore likely to have addressed such issues, were approached via phone and email with a view towards obtaining organisational documentation which addressed those questions identified on the survey instrument.

Principal findings
Literature review
A review of pertinent literature identified four major areas of importance for administering electronic patient data:
1. Patients’ right of ownership to electronic patient records.
2. Custodial issues with data stored in centralised health care institutions
3. IT Security, including hierarchical level access, data encryption, data transfer standards and physical security
4. Software applications usage.

Survey development
After the legal and ethical standards were reviewed, we identified eight areas of concern where identification of best practice required further investigation. A single question was devised to address each of these areas for the purposes of the survey, and these fell under three major headings:

Accessing datasets of patient information
1. If patients do not specifically consent to the use of their data for reasons unrelated to their personal treatment (such as for research purposes), what is your organisation’s position on requests for this data from external organisations?
2. How do organisations define levels of anonymity if patient databases are being given out to third parties (e.g. for research). Does your organisation have standards or protocols for the de-identification of patient data when databases are being supplied for research purposes, in order to retain patient anonymity? Do you have protocols for handling requests for different levels of data de-identification?

Accessing individual patient information
3. How does your organisation decide what level of access to electronic patient information will be given to different types of staff (e.g. what should a physiotherapist or dietician or junior doctor need to access?)?
4. If an external healthcare organisation becomes allowed to access your organisation’s electronic patient databases, what limitations are put on the data they may access? Can they access details of patient episodes dating from prior to when they became allowed to access your databases?
5. Does your organisation have a policy of making patients aware that their data might be used for secondary purposes such as research?
6. Does your organisation have a policy about what constitutes a reasonable effort to ensure patient consent for collection, storage and use of data? What if the patient is unable to give consent at the time of admission?

Security of the IT system
7. What standards are in place for encryption of transferred information and hardware/device security in order to protect patient information being stored electronically by your organisation?
8. What is the core software application used by your organisation to manage patient databases and share information across departments or with external health providers?

Discussion
Surveys have been sent to fourteen health care organisations requesting documentation relating to these issues mentioned in the survey. Collation of these results will provide us with a greater understanding of accepted practice standards in the use of electronic patient data.

Implications for policy, delivery or practice
This literature review has underlined a gap between the laws which govern medical records and the actual ethical practice which is undertaken in health organisations. We hope this study will indicate to health institution administrators the requirement for sufficient governance when dealing with securing medical data electronically.

References

Acknowledgements
This research was supported with funding from the Australian Government Department of Health and Ageing, through their Primary Health Care Research Evaluation and Development program at the Greater Green Triangle University Department of Rural Health. We would like to acknowledge the involvement of the hospitals for their time and valuable information provided towards the completion of this project.

Date of Poster Publication: July 2006