				password choice
Database	Security compromised (general)	Data leak to non-medical people	Expensive, especially if technical failure	Database security may be applied (details not relevant here)
	Security compromised via network	Loss of d/b availability	Inconvenient	Firewall
	Security compromise leading to disk "crash"	Significant downtime and major loss of data	Catastrophic; possible loss of project data mine	Nightly/daily tape backup routine
Hand-held wireless data system	Wireless data connection compromised	General loss of confidentiality and integrity	Embarrassing	Secure transmission of data (involves consideration of crypto algorithms and protocols)

C.2 Security policy

In [5] Ross Anderson describes the security policy, given in the Appendix, below, that the British Medical Association used to govern access to medical information systems. The "BMA Model" describes a convention for setting out the rules about how information may flow between the various entities in the medical system. The BMA model supports a decentralized system that takes into account the need of the data subjects to make access control decisions. This improves on the Bell-LaPadula model in which access control decision making is centralized and the lattice model which compartmentalizes data but does not show how to manage the flow of information.