Security Part II 2005 P1 Q4 RJA

(a) Medical records can be protected by the BMA policy, or by a role-based access control system that localises exposure using rules such as 'a nurse can see the records of any patient who's been in her ward in the previous 90 days'

(b) Police intelligence data are traditionally managed using multilevel-secure systems with compartmentation by codewords, although at the compartmentation level a policy such as BMA or RBAC can be used too

(c) School records have mostly got integrity requirements, though some entries may be highly sensitive (disciplinary matters) and others may involve specially sensitive data in terms of the Data Protection Act

The problem posed by the Children Act is how to devise a policy that is a refinement of each of the above simultaneously. One approach would be to evolve a BMA variant or RBAC system acceptable to the police. Another, in the case of medical flows to a system containing police data, would be to devise a codeword to create a special compartment for the new material. Yet another approach might be 'system high' in which all the merged data were Top Secret. Most of the practical problems will come from aggregation (which localisation via RBAC doesn't really solve). There will also be feature-interaction and policy-conflict issues, and no doubt covert channels. Finally, there will be problems of assurance at both the technical level and the professional level.