

Appendix A

Policy ADM-c-140

Classification of Information Security Breaches

Classification	Information Type	Harm
1 – Low sensitivity	<ul style="list-style-type: none"> • Basic personal information, e.g. patient registration numbers, photographs of individuals, dates of birth, staff member salaries • Policies or proposals for decisions not yet completed 	<ul style="list-style-type: none"> • Erosion of CapitalCare credibility as a service provider • Exposure of individual without consent • Risk of misperception of individual or CapitalCare
2 – High sensitivity	<ul style="list-style-type: none"> • Sensitive personal information, e.g. patient diagnostic and treatment information, personnel records, quality assurance committees • Third-party business confidences • General Ledger, client trust and ward account information • Sensitive business documents 	<ul style="list-style-type: none"> • Serious injury to privacy of individuals • Substantial economic harm to third parties or CapitalCare • Compromise of CapitalCare disaster preparedness and recovery
3 – Extreme sensitivity	<ul style="list-style-type: none"> • Information deemed extremely sensitive such as narcotics medication, diagnosis or communicable diseases, keycodes to locked units, user account and password information required to gain access to systems containing large amounts of health information • Information on how to gain access to client homes • Information describing security systems and mechanisms 	<ul style="list-style-type: none"> • Immediate threat to health and safety of patients, staff or others • Threat to security systems protecting medical facilities and equipment