



Information Disaster Recovery Plan

The increasing reliance on electronic information highlights the need for backup systems (disaster recovery plan) to enable continuity of practice in the event of an information disaster such as a fire or power or equipment failure.

The plan shall include all of the following sections.

GENERAL INFORMATION

Provides general information in regards to computer security. Ideally this would include the computer security policy, asset register, delegation of responsibilities and contact details for applicable companies and persons.

POTENTIAL DISASTER PLAN

POTENTIAL DISASTERS: Power failure, System or file corruption, Internet disruption, etc.

For each 'Potential Disaster' the Practice should have a contingency plan. Each plan should be comprehensive and describe to appropriate staff what immediate action should be undertaken (eg. contact Internet service provider, check power supply, run antivirus software etc).

CRITICAL FUNCTION PLAN

CRITICAL FUNCTIONS: Appointment system, Accounts/billing system, Medical Records, Referrals letters, Prescriptions, etc.

'Critical functions' are those that would still need to operate in the event of a disaster. All critical functions should be identified, both administrative (eg. appointment system, billing system) and clinical (eg. consultation note recording, blood pressure monitoring and recording) and should have a comprehensive contingency plan, describing what action to take to ensure the 'critical function' can still operate.

SYSTEM RESTORATION PLAN

Once the contingency plans have been completed and the disaster is over, the Practice needs to implement systems to restore the Practice to normal operations. Restoration plans could include: re-installing software, reinstating electronic appointment system, and restoring computerised patient health records.

Once again, each area that will need to be restored will require a comprehensive plan.

TESTING OF THE PLAN

Once each contingency plan has been developed, the Practice should test to ensure functionality. Then, to meet the criteria of the standards, the plan and test will be documented.

REVIEW AND ASSESSMENT OF THE PLAN

Once the disaster is over or the testing is complete, the Practice should assess the recovery plan, and any response, to ensure it is appropriate. This would include assessment of the reason for the disaster, how the recovery was done, if the current system requires updating and any issues that may have arisen.

GPA ACCREDITATION *plus* has developed an Information Disaster Recovery Plan Template for Practice use. This has been developed as a guide only and should be personalised to each individual practice. Please contact GPA for your copy.