

COMPUTER SECURITY CHECK-LIST

This is a check-list for you to see whether you have put in place a number of computer security processes or systems. Please note that the list is restricted to security aspects of IT. The guideline describes each item in the check-list in more detail.

IT CATEGORY	TASKS	HAS THIS BEEN IMPLEMENTED: (TICK IF YES)
Practice computer security coordinator	<ul style="list-style-type: none"> Practice IT security coordinator's role description written (for GP, existing staff member or practice manager) Practice IT security coordinator appointed IT security training for coordinator provided Security Coordinator's role reviewed on... 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="text" value="/ /"/>
Practice IT security policies and procedures	<ul style="list-style-type: none"> Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual) IT security policies and procedures documented IT security policies and procedures documentation last reviewed... Staff trained in IT security policies and procedures 	<input type="checkbox"/> <input type="checkbox"/> <input type="text" value="/ /"/> <input type="checkbox"/>
Access control	<ul style="list-style-type: none"> Staff policy developed on levels of electronic access to data and systems Staff have created personal passwords to access appropriate level Passwords are kept secure Consideration given to changing passwords periodically 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Disaster recovery plan	<ul style="list-style-type: none"> Disaster recovery plan developed Disaster recovery plan last tested... Disaster recovery plan last updated... 	<input type="checkbox"/> <input type="text" value="/ /"/> <input type="text" value="/ /"/>
Consulting room and 'front desk' security	<ul style="list-style-type: none"> Practice aware of need to maintain appropriate confidentiality of information on computer screens Screensavers or other automated privacy protection device enabled 	<input type="checkbox"/> <input type="checkbox"/>
Back-ups	<ul style="list-style-type: none"> Back-ups of data done daily Back-ups of data stored offsite Back-up procedure last tested (by performing a restoration of data)... Back-up procedure has been included in a documented disaster recovery plan 	<input type="checkbox"/> <input type="checkbox"/> <input type="text" value="/ /"/> <input type="checkbox"/>
Viruses	<ul style="list-style-type: none"> Anti-viral software installed on all computers Automatic updating of viral definitions enabled (daily if possible) Staff trained in anti-viral measures as documented in policies and procedures manual 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Firewalls	<ul style="list-style-type: none"> Hardware and/or software firewalls installed Hardware and/or software firewalls tested 	<input type="checkbox"/> <input type="checkbox"/>
Network maintenance	<ul style="list-style-type: none"> Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches) Uninterruptible Power Supply installed (to at least the server) 	<input type="checkbox"/> <input type="checkbox"/>
Secure electronic communication	<ul style="list-style-type: none"> Encryption systems considered Encryption used for the electronic transfer of confidential information 	<input type="checkbox"/> <input type="checkbox"/>