BASELINE GENERAL PRACTICE SECURITY CHECKLIST

PATIENTS FIRST
Better Health with Better Systems

#	Question	SELF (Y/N/U)	INDEPENDE NT (Y/N
1	Are all computers with access to health information running operating systems that are currently supported with security patches?		
2	Do you use a paid third party IT specialist to undertake or have oversight of your IT. Note that people providing this service unpaid, e.g. friends or family don't meet this requirement. (1)		
3	Do your practice policies cover acceptable use of information and systems by staff? (2)		
4	Do you take at least daily backups of your system.(3)		
5	Do you store backups securely off-site either through a paid online system or through a professional off-site archiving company? Note that staff taking backups home doesn't count and free online storage e.g. Dropbox doesn't count. (3)		
6	Have you ever tested your backup restoration process? (3)		
7	Do your staff have access to only the information that they need and no more within the PMS (e.g. Reception staff can't access clinical notes in the PMS). (4)		
8	Is your PMS server secured against theft after-hours (e.g. in a separate locked, entry proof location) OR your PMS is in a hosted data centre. (5)		
9	Do your staff always send patient information using secure means? Note that sending by plain email is almost never secure. (6)		
10	Does your server have critical security updates and patches applied at least every month? (7)		
11	Do all computers in your practice require a password to access them from start-up? (8)		
12	Do all computers 'lock' after no more than 15 minutes of inactivity? (8)		
13	Do all computers in your practice have anti-virus software installed, running and updated regularly? (9)		
14	Does your practice have a documented plan for disaster recovery and business continuity that addresses patient health information and the ongoing operation of the practice if your information systems are unavailable for an extended period. (10)		

This checklist is based on principles from the Health Information Security Framework (sections shown in bracketed numbers after each item). It should be used as a primer for ensuring that you have good processes and practices in relation to the way you secure and use health information. It does not represent a comprehensive security assessment or plan; please refer to the full Health Information Security Framework for more information.

Last Updated 11 November 2016