Doi: http://doi.org/10.1027/1015-5759/a000606

Supplementary Material 1: Security protocols for home-based work arrangements

The following security guidelines were written based on NUH CDU's institutional guidelines and serves as a reference guide for design of similar protocols in other institutions. They may not however be fully applicable to other institutions and security guidelines should be adjusted according to current local legal regulations.

Protocol security

Protocols code list will be maintained by each psychologist (password protected)

Full name	Code	Type	Date removed	Date returned
XXX	(Internally decided)	e.g., ADOS M1		

After completing assessment, psychologists bringing protocols home should:

1. Assign a code.
2. Enter the code into the protocols code list.
3. Write the code onto the physical protocols in ink.
4. Write the assessment date and place psychologist name stamp.
5. Place protocols in an official organisational A4 envelope with clinic stamp and psychologist name stamp.
6. Protocols should not be left unattended in transition to and from office.
7. Protocols should not be placed in public spaces – report writing should be completed within the confines of a home.
8. Upon returning the protocols to the office, update the protocol code list, place patient name sticker on the protocols and file as usual.

Doi: http://doi.org/10.1027/1015-5759/a000606

9. Should protocols be stolen, please report to your Supervising Officer immediately.

Report security

1. Reports should be written on hospital-issued laptops only.
2. Reports should be saved only in the encrypted documents folder in the work laptop.
3. Reports should be password protected with an internally developed code.
4. For file transfer, please use institutional email, institutional cloud drive, or institution-assigned external hard drive.
5. Laptop security measures should adhere to institutional guidelines.