October 2017

THE MANAGEMENT AND STORAGE OF RESEARCH DATA

Scenario

Dr A and his research team are conducting a study on the prevalence of disease XY in Singapore. The collected research data is stored in a password protected folder in a shared drive in their institution's network for ease of access.

Six months on, a ransomware attack exploited a security flaw in the institutional computer software.

After this attack, Dr A was unable to determine if there was unauthorized access to the patient data, which can have damaging effects. Potentially compromised data included subject names, referral, treatment dates and procedures received. This incident also led to the institution reviewing its data security procedures as it assesses the extent of the data breach.

What should have been done to prevent the incident?

- Electronic databases should be password protected and preferably stored on stand-alone computers rather than on the common drive. [1]
- The databases should not contain subject identifiers and the data linking subject identifiers and the subject identification codes should be stored separately. [1]

Some useful IT pointers to follow:

- Safeguard data, personal information, sensitive/confidential information. [2]
- Do not share your usernames and passwords/ authorisation codes with anyone.
- The integrity of software and data should be safeguarded. Detection and prevention controls to protect against virus and malicious software should be implemented. [3]
- Exercise due care for all removable storage devices (e.g. USB drives) containing confidential information, to avoid theft and loss. [4]
- Report security breaches or suspected security events and take necessary corrective actions as stated in the organisational policies. [4]

Considerations for the Storage of Data

The hypothetical incident above shows the importance of keeping up to date with the latest software security patches as well as the importance of regularly reviewing data security policies.

References:

1. **NHG Proper Conduct of Research SOP – 501-B08 Data Collection and Handling**
2. **NHG User Guide for IT Usage and Information Sharing**
3. **NHG Policy on IT Security, Version 2.3**
4. **Healthcare IT Security Policy and Standards Version 3.0**

Article Contributed By:
Mr Nantha Kumar, IRB Analyst,
NHG Domain Specific Review Board
Edited By: NHG-RDO