Secure handling and data destruction policy:

1. Overview:

Secure data handling and data destruction is a key aspect of ensuring patient-doctor confidentiality. Insecure handling of data or improper data destruction can lead to this data being accessible by third parties outside of either the relevant patient or Wellington hospital. This would break the Health Information Privacy Code of 1994.

2. Purpose

The purpose of this policy is to establish a guideline for the secure handling and destruction of physical and digital data for hospital employees. This covers what is deemed to be sensitive data, how the data is to be shared and the best practices for internal and external technologies/devices that interact with the data.

3. Scope

This policy identifies the information as being sensitive and also provides guidelines how employees of Wellington Hospital (exclusive of contractors) handle the data and also destroy it. This involves both hard copy and soft copy handling and destruction of sensitive data.

4. Policy

4.1 Destruction of physical documents should be done using the standard shredder (mention). Classified documents should be shredded using a line shredder, highly classified should be destroyed using cross cut shredder
4.2 Portable and external storage devices must not used and are not allowed to be connected to local systems within Wellington Hospital.
4.3 Digital data must be stored in the correct locations that have access restricted to the relevant groups, see relevant access control policy
4.4 Allow ocertified health professionals with permission to access confidential data remotely through encrypted and secure channels. They must only use devices given to them by Wellington Hospital for this. To access this information remotely two factor authentication must be used, see the Remote Access policy for more information. Connection must occur through VPN, and under no circumstances use open-internet.
4.5 All physical data must be locked in cabinets when not being accessed. Digital data must be stored and restricted following relevant access control policies
4.6 All personnel must follow the clean desk policy, and must not leave any physical documents on their desks unattended
4.7 Medical practitioners (Doctors, nurses) of Wellington Hospital can email patients about their own medical history, and doctors can be able to access information about the relevant patient. They cannot access information outside of the patients that they are assisting
4.8 Wellington Hospital will monitor access to all data.
4.9 No physical documents must leave Wellington Hospital.

4.10 Employees must not share any sensitive information with anyone apart from the specific, corresponding patient.
4.11 Any sensitive data stored in the cloud must remain in New Zealand
4.12 Staff can only create documents with the appropriate permissions.
4.13 All data should be created, made, accessed and modified with a confidentiality level in mind. This confidentiality level should be listed at the top of the document.
4.14 Patient information should be accessed on a need to know basis
4.15 Medical practitioners can obtain access for the medical records of the patients they are treating.
4.16 Patients identity needs to be checked before any information can be provided or released to them
4.17 All digital data cannot be stored locally on a device's hard-drives. It must be stored on one of the Wellington Hospital servers or databases
4.18 CDs and DVDs must be shredded to a size smaller than 1mm squared
4.19 Employees must comply with the password policy for any devices and accounts that interact with sensitive data
4.20 Hard-drives and removable media must be wiped following Bruce Schneier's Algorithm, so that no data recovery methods can retrieve previous information stored on those devices.
4.21 Employees must not leave information or devices unattended at any time.
4.22 No sensitive information should be shared via personal emails and unofficial email clients
4.23 Wellington hospital employees must use work email accounts for all work related emails
4.24 Sharing sensitive information between Wellington Hospital employees must be done via the approved methods outlined by the Wellington Hosptial information security officer
4.25 Network printers and scanners must be wiped when they are no longer to be used by Wellington Hospital. Their hardrives must be wiped and follow 4.20.

5. Policy Compliance and liability
Employees who violate these policies may have appropriate actions taken towards them i.e. immediate termination or suspension actions. Note that if the action is found to be criminal in nature immediate termination will be taken and all supplementary actions the law will be taken against you and not the company

6. Related Standards, Policies and Processes

7. Definitions and Terms
Secure data is the patient and employee information stored by the Wellington hospital. This information includes name, age, contact details, medical history, and any other personal information.

Medical practitioners - Doctors, surgeons, nurses.

8. Revision History

Date of Change	Responsible	Summary of Change
29/07/2020	Cybr373 Students	Creation

Members:
Max Shallcrass
Jaimee Mullins
Harrison Compton
Lavanya Sajwan
Lane Huffman-Devey