Neurocode Policy for Protection of Personal Information and Confidentiality

1. Introduction and Scope

Neurocode is committed to providing our clients with highest level of confidentially. This includes protecting the privacy of all personal and confidential information in our care. When handling personal information, Neurocode abides by the UBC Protection of Personal Information and Confidentiality Policy. https://universitycounsel.ubc.ca/files/2017/05/Fact-Sheet-Overview-of-Privacy.pdf This link should be reviewed by all staff on annual basis.

The purpose of this policy is to define a document control system to assure that:

1.1 A guiding principle and framework is established for Neurocode and its Staff to comply with regards to managing Personal and Confidential Information.

1.2 Accountability for managing Personal and Confidential Information is demonstrated.

1.3 Trust-based relationships with clients, Staff, business and healthcare partners.

This Policy applies to all Neurocode Staff relating to Personal and Confidential Information, regardless of the format of the information. Neurocode lab is not open to the public; we have no facilities to perform sample draws from patients.

2. Policy

Neurocode and its Staff will comply with the professional codes of ethics and standards of practice, and applicable legislations such as the BC Freedom of Information and Protection Privacy Act (FIPPA) and the Personal Health Information Access and Protection of Privacy Act (e-Health Act).

All Staff are responsible for compliance with this Policy as well as other applicable laws, professional codes of practice and contractual obligations in collecting, accessing, and disseminating Personal and Confidential Information.

2.1 Confidentiality Undertaking

As a condition of employment or affiliation, all Staff must mandatorily read the Neurocode Information Privacy and Confidentiality Policy and acknowledge their understanding of the obligation to protect private information by signing an approved Confidentiality Undertaking

form or other agreement as deemed appropriate by Neurocode. All Staff are required to reaffirm their understanding of and commitments to upholding confidentiality on an annual basis.

The training record must be retained for three years by Lab Manager to ensure protection of personal information and confidentiality compliance.

2.2 Privacy and Confidentiality Education

Upon employment, Staff must complete mandatory privacy and confidentiality education as determined by Neurocode. The privacy education will be determined based on Staff roles and responsibilities.

2.3 Collection and use of Personal Information

Staff may collect Personal Information as needed to perform tasks. Where possible, Personal Information will be collected directly from the individual that the information is about. At the time of the collection, the individual should be informed of:
- the purpose of the collection
- the legal authority for the collection; and
- the contact person information if the individual has any questions about the collection

Staff may access and use Personal Information for legitimate purposes on a need-to-know basis in order to perform job functions and responsibilities.

2.4 Disclosure of Personal Information

For an overview of Disclosure of Personal Information and requirements governing the security of personal information, refer to the UBC Information Security Standards. https://cio.ubc.ca/information-security/information-security-policy-standards-and-resources#user_standards

2.5 Accuracy of Personal Information

Neurocode and its Staff will take reasonable steps to ensure the accuracy and completeness of any Personal Information they collect or record and take extra measures to protect against making any errors due to carelessness or other oversights.
Medical Director is responsible for updating and maintaining the accuracy of personnel records. Staff should direct any clients requesting correction or amendment of information in their medical records to Medical Director.

2.6 Retention and Destruction of Personal Information

Personal and confidential information must be retained for three years.
For the safe destruction of Personal and Confidential Information stored digitally or electronically must be physically or magnetically erased. Encrypting or overwriting the information is insufficient due to the possibility of it being recovered.

Personal and confidential information should never be stored on a personal digital device due to the software's ability to reconstruct deleted data. If any personal or confidential information is stored on a personal digital device, contact Information Technology to arrange for cleaning of the hard drive.
All physical documents containing personal and confidential information must be discarded into the designated shred-it containers. Documents containing private information cannot be discarded with regular garbage or in recycling bins.

2.7 Protecting Information

Neurocode Staff should take reasonable precautions to ensure that all Personal and Confidential Information is protected against unauthorized access, collection, use, disclosure, or disposal.

2.8 Reporting Privacy Breaches

Any suspected breach of privacy or violations of this Policy including the theft or loss of Personal Information, devices or paper records must immediately be reported to the Medical Director. For more information about how to deal with a privacy breach, refer to the Fact Sheet "Handling Privacy Breaches".
https://universitycounsel.ubc.ca/files/2015/05/Fact-Sheet-Handling-Privacy-Breaches.pdf

2.9 Challenging Neurocode's Compliance to Policy

Neurocode will investigate all concerns from individuals regarding compliance with this Policy. If the complaint is found to be justified, appropriate measures will be taken, including amending policies and procedures, if required. The individual will be informed of the outcome of the investigation.

2.10 Compliance

Failure to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment, or loss of privileges.

References

1) BC Freedom of Information and Protection of Privacy Act (FIPPA)
2) https://universitycounsel.ubc.ca/files/2017/05/Fact-Sheet-Overview-of-Privacy.pdf
3) E-Health (Personal Health Information Access and Protection of Privacy) Act
4) Providence Health Care CPF0300: Information Privacy and Confidentiality Policy