CNTH Pathology
Department of Chemical Pathology,
CNTH, Ragama, Sri Lanka

Information Technology (IT) User Responsibilities for the Doctors registering for CNTH Pathology online access

It is mandatory that all medical professionals using the CNTH Pathology online system strictly adhere to the following.

1. Responsibility of the user for his/her account security
   1.1. Users are responsible for the security of their credentials and should take reasonable precautions to prevent others from misusing their credentials.
   1.2. Under no conditions must a user provide his or her password to another person.

2. Confidentiality of information
   2.1. According to the Guidelines on the Ethical Conduct of Medical & Dental Practitioners Registered with the Sri Lanka Medical Council, although there is no specific statutory provision, confidentiality is implied in the contract between a doctor and a patient.
      2.1.1. Users must ensure that the information obtained from CNTH Pathology remains **strictly confidential** and is not divulged to any third party except where required for clinical reasons or by law.
      2.1.2. Any unauthorized disclosure of patient information obtained from CNTH Pathology would constitute a breach of contract with grounds for civil proceedings against the doctor.
      2.1.3. Any information obtained from CNTH Pathology must be disclosed to a third party not involved in the patient management **only with** written valid consent for such disclosure.

3. Unlawful or destructive activities
   3.1. Users shall not use the CNTH Pathology for any purpose that violates the law or threatens the integrity of the system.
      3.1.1. Users will not attempt to gain unauthorized access to the system or go beyond their authorized access. This includes attempts to log in using another user's credentials and attempting to override any security functions.
      3.1.2. Users will not intentionally develop or use programs to harass other users or to attempt to violate the security or alter software components of any other network, service, or system. Examples of such activities include hacking, monitoring, or using systems without authorization, scanning posts, conducting denial-of-service attacks, and distributing viruses or other harmful software.
      3.1.3. Users will not attempt to damage hardware, software, or data belonging to the organisation or other users. This includes adding, altering, or deleting files or programs on local or network hard drives and removing or damaging equipment.

Name : _____ SLMC:_____
Date : _____