# NRR Information Security Policy

## Introduction

This document has been produced to ensure that:

- A higher level of security in terms of patients' information confidentiality, centre confidentiality, integrity and availability of data information is maintained at all time.
- All sites users and site coordinators are aware of their authority and accountabilities as stated in the NRR Authorization Form.
- All site users are aware of that NRR is governed and operated based on various approvals and policies such as Personal Data Protection Notice and Privacy Policy which are available in the NRR Website and thus should ensure compliance with the stipulated policies.

## Management

### A) User Level

1. Provide true and up to date information about yourself to the registry in the MyProfile page
2. Do not disclose your user ID or password to anyone else. Each of the activity in the web application has an audit trail.
3. Do not give your mobile phone to anybody else while logging into the web application.
4. Log in the pin number immediately after receiving the number via SMS.
5. Users are responsible to update/edit their own centre data.
6. Should the user lose his/her mobile phone or change a new mobile phone number, he/she should inform the Doctor in-charge / Site Coordinator who shall than officially inform the NRR coordinator via web. (Document: User –Change Details Link)
7. Should the user forget his/her password, please login at the **Forgot Your Password** at the main page of the web application. It is compulsory for user to provide correct registered login 'User Name' and "e-mail address' or 'mobile phone' for verification. The password will be sent via mobile phone.
8. Please read password management as per Appendix A (Security Practices)

### *B) Centre/Institution Level*

1. Provide true and up to date information about my centre to the registry in the Centre Information / Centre Survey page
2. Agree to allow other authorized users within the same institution as per Authorization List for their specific responsibilities.
3. Ensure that your database is updated regularly to maintain its real-time accuracy.
4. Agree to share aggregate data from your centre for the purpose of research by qualified researchers, or for any other purpose by persons demonstrating a need

to access the NRR web application (s) following approval by the NRR Advisory Committee.

5. The SDPs hold sole responsibility with regards to release of own patients' data to any party concern. NRR would appreciate a notification of the purpose and details where applicable.



[ ] I hereby ACKNOWLEDGE and ACCEPT that my access and use of the NRR Web applications shall be governed by this Security Policy.

# Appendix A

## *Security Practices*

As a good security practice you are strongly advised to:

Keep your password confidential!

- Avoid sharing or divulging your Password to anyone. This includes any person who may appear to represent or work for the Registry. Our administrator never require your password at any time.
- Avoid using the same Web Application Password for any other web-based services such as for e-mail or for Internet Service Provider login.
- Avoid choosing a Password that is easily anticipated by a third party, like your NRIC number, telephone number, date of birth, etc. You should select a unique Password to make it difficult for anyone to anticipate.
- Avoid writing down or saving your Password on your browser or any other software. Memorize your Password.
- If you suspect your Password may have been compromised, change your Password immediately.

Ensure you are accessing the correct website!

- Never access the website via a hyperlink from an e-mail. Always enter the correct website address yourself.

### Only access Web Application using a secure and trusted computer!

- Never access your Web Application on Computers/devices that you have doubts with regard to security, such as those located in public places. If you have to use computers (for example, when you are on trips), change your password once you have access to a secure computer.
- Keep your operating system (eg. Microsoft Windows) and Internet-related software updated with the latest security patches.
- Protect your computer from viruses and malicious programs with anti-virus software and firewalls where possible. Always update your anti-virus software with the latest virus signatures.
- Always log out your online session by clicking on the “logout” button whenever you leave your computer, even for a short while. Do not simply close the browser window when you wish to end the Web Application session.

For further information on the above, or any aspect of Internet security, please contact our Administrator helpdesk as stated in http://www.msn.org.my/nrr/contact.jsp