Data protection and Ethics regarding the ESID Database

Documents necessary for documenting in the ESID Database

- Patient consent form signed by the patient or legal guardian (please refer to the ESID web site for the latest available version)
- Positive ethics and data protection statements as required by local authorities
- Agreement between ESID and documenting centre signed
- For the coded version of the database: A list matching patient ID with the ESID-database ID. This is your responsibility and it must be kept secure. We do not have this information.

General Security Measures for Protected Health Information

- Use strong passwords, but do never share them
- Lock doors, lock file cabinets, and limit access to workspace where health information is used or stored
- Limit access to printers and fax machines where health information is printed
- Limit access to health information to only those who need it for a specific task
- Use de-identified health information whenever possible
- Shred or otherwise properly dispose of health information trash
- Use and keep only the minimum health information necessary for a specific task
- Follow local privacy policies and procedures

Database Security Measures

As a user, you are responsible for making sure no one else can access the database by using your login name and password!

- Keep login and password secure. **Never** tell anybody your user name or password!
- **Never** allow your internet browser to store your login name and password! Otherwise, anyone else using your computer will be able to log in.
- Keep your system up-to-date.
- Keep Malware-Scanners ("Anti-virus software") up-to-date and **use** them regularly!
- Enter data from a computer within your institute's firewall rather than from home. Do not use public internet access points.
- We recommend using Firefox or Chrome
- Please make sure you are really on **https://cci-esid-reg.uniklinik-freiburg.de**
- You can set a bookmark in your browser to avoid typing errors.
- **The site is SSL encrypted so there is a little**  **visible on your screen.**
- **Don't get fooled by phishing mails!** Phishing mails often direct you to spoofed (fake) websites via embedded links within the email. These sites may look identical to the original database login-page.
- Beware of messages from ESID asking for your password. We **never** request your password.
- Do not open any e-mail attachments unless you are sure they are ok.

Password rules:

The password you receive from us must be changed as soon as you log on to the ESID database. It must be:

- Minimum of 8 digits
- Combination of lowercase, uppercase letters, numbers and special characters
- Must be kept secret at all times
- Must not be used elsewhere and should be changed regularly

For security reasons: If the password is entered incorrectly several times, you cannot access the ESID database for a given time. Further security measures take place if more incorrect passwords are entered. If you lose or forget your password please contact us at esid.registry@kenes.com for a new one.