St. Jude Global SJCARES

Security FAQ: Keeping Your Data Safe Using the SJCARES Registry

What program and/or company does St. Jude Children's Research Hospital work with to provide the SJCARES Registry?

The SJCARES Registry is developed using the OmniComm TrialMaster platform. Omnicomm is a leading eClinical solutions company that supported clinical trials and registry work around the globe. We also are happy to note that clinical trials sponsored and run by investigators at St. Jude Children's Research Hospital use the same platform.

How does OmniComm and St. Jude Children's Research Hospital protect my data in the SJCARES Registry?

- OmniComm performs security monitoring of registry instances on St. Jude's behalf. If potential security incidents are detected, OmniComm alerts St. Jude so action can be taken.
- OmniComm maintains compliance with 21 CFR Part 11 and makes available to St. Jude attestation reports to its compliance.
- OmniComm maintains formal disaster recovery plans and procedures. St. Jude has a designated contact whom OmniComm notifies in the event it is triggering DR failover procedures.
- Data transmissions of data between an Alliance Member program and the TrialMaster service uses HTTPS encrypted communications methods.
- Regular external audits of their data centers physical and logical security measures and practices.
- Logs are maintained for any access of records in the solution.
- Breach notification – If OmniComm's service is compromised or if OmniComm informs us of any activity that would indicate that a site's data has been accessed by an unauthorized party, we will report this information to a site's coordinator within 72 hours of this notification or discovery as dictated in the terms of the data use agreement.

How will I log-in to Omnicomm TrailMaster and is it secure?

- Access to OmniComm TrialMaster is controlled on a per-registry basis. Each registry uses role-based access controls, with roles designed during registry setup to enforce least privilege.
- All access to a registry instance within OmniComm TrialMaster requires authentication using a valid username / password combination. OmniComm encrypts all passwords in storage.
- In addition to the security measures of the OmniComm TrialMaster platform, user accounts are secured via complex password pattern requirements, forced password changes at a regular interval.

- Site and role-based security: In addition to data segmentation, site level permissions and user security roles in TrialMaster are used to define levels of access.

Are data from my registry mixed with data from other studies and/or Alliance Members?

- St. Jude's trials data is segmented and housed on separate servers and is not co-mingled with other OmniComm clients. In addition to this server level segmentation, your data is segmented from other sites in the registry by the security and data protection measures designed in TrialMaster.

How are personal health identifiers managed to ensure compliance with data privacy laws?

- Any access by support staff in the Department of Global Pediatric Medicine at St. Jude Children's Research will have personal health identifiers (any names, national IDs, reference IDs, any address fields) hidden and not viewable by St. Jude staff. Only staff at the Alliance Member site for a particular registry instance can view personal health identifiers.

I see I will own the data at my center but are my data also being shared with others?

- Data use rights are defined in the data use agreement signed by both the sites and St. Jude Children's Research Hospital. We do not share a site's data without their explicit permission and the conditions and requirements for data sharing are detailed in the data use agreement. We do ask for site permission to deidentify data and house the information in a global distributed data warehouse. The academic benefits of participating in this system are spelled out in the data use and transfer agreement.

What can you I do to help keep my data safe?

- Keep your software (operating system and applications) updated. Run supported versions of software that receive periodic updates to address security issues and vulnerabilities.
- Use a screen locking solution to control access to your system when you step away from the computer.
- Run antivirus on your computers and keep this software and its virus definitions up to date. Use a firewall solution on the computer.
- Limit non-business use on system used to access the SJCARES Registry.
- Limit who has administrative access to systems.
- Be careful when installing applications or browser plug-ins. Install solutions only from trusted sources.