Fast Facts for Families
Data Privacy and Security

Do you have questions about privacy and security of your data within the ASQ® Online system? Read this Q&A to learn how we ensure the safety of your family's information.

Is ASQ Online safe to use?

Yes. As publisher of ASQ, Brookes is committed to keeping your child's and family's data safe, secure, and private. ASQ Online uses robust physical and technical security safeguards to protect all child and user data entered into the system—and ASQ Online complies with both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Family Educational Rights and Privacy Act (FERPA). See the next page for an in-depth look at security measures in place.

Who has access to data about my child and family?

Data is accessible to the provider assigned to your child and family. This may be your child's pediatrician, teacher, home visitor, or other professional. The administrator for the program or account also has access and determines who else can see your information. In some cases, the program may choose to share data with a larger entity, such as a state or school district. Data about your child and family may continue to be accessible after your child leaves the program. To learn more about how your data will be used, please reach out to the provider or organization that invited you to complete the ASQ screening.

Do Brookes Publishing employees have access to my child's data?

Brookes employees do not have free access to child and family data in ASQ Online accounts. In rare instances, an employee may be given temporary permission by the program to view data solely to resolve technical issues.

Will my data be used in any research?

In some instances, Brookes Publishing and the ASQ authors may use child and caregiver data, which is stripped of all personally identifying information about individual children, families, providers, and programs, for research purposes.

Have any other questions? Please contact us at implementation@brookespublishing.com

How Your Child's Data Is Protected in ASQ Online

ASQ Online uses robust security measures to protect your data, control access, and ensure confidentiality. Here is a closer look at the specific security measures we use to safeguard your child and family data:

Network Security: Browser-level encryption protects all your confidential data and information. ASQ Online uses SHA-256 Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, which is also used by most financial, medical, and educational institutions to protect data from interception during transmission. SSL prevents unauthorized access to your data.

Access Security: Our servers are protected by industry-standard firewall technology. Only authorized traffic and requests from legitimate sources are allowed through the firewalls to ensure the safety of your data and our server equipment.

Data Security: Your information is stored in a secure data center using industry-recognized security safeguards, such as firewalls, coupled with carefully developed data security procedures that defend your information from loss, misuse, or unauthorized alteration.

Physical Security: Our databases and servers are in a secure data center that includes robust physical security, conditioned power, environmental controls, uninterruptible power supplies, and fire suppression technologies.

Password Security: Users can only gain access to the system by providing a valid username and password combination, which is encrypted while in transmission.

If you complete questionnaires online through ASQ Family Access, our protocols ensure that the information you provide is secure from interception during transmission and prevent unauthorized access to your data. Any data you submit can be viewed only by those who have authorized access and have been assigned a role that allows them to view your child's and family's data.

Have any questions? Please contact us at implementation@brookespublishing.com