Data Security Documentation

Hardware Security

Security	• 24x7x365 magnetic card key access with secondary biometric authentication • 24x7x365 onsite security personnel • Hardware is housed within interior of building with no direct exterior access • 24x7x365 on-site staffed Network Operations Center (NOC) • Digital security cameras and intercom system • Power delivery infrastructure, generator, diesel fuel and telecommunications infrastructure maintained in secured underground concrete vault
Fire Detection & Suppression	• Certified data center smoke detection system • Clean agent fire extinguishers placed throughout facility • Dual-Interlock Pre-Action dry pipe sprinkler system
Power	• Four 300 KVA UPS Systems • Triple battery strings • 1.5 Megawatt diesel generator • 6,000 gallon diesel fuel supply (with first rights to fuel if a disaster occurs) • Dual ATS (Automatic Transfer Switch) • Multiple redundant Power Delivery Units (PDU)
HVAC/ Environmental Design	• 140 Tons (7, 20 Ton units) of AC keep environment at constant temperature and humidity with cooled flooring • Anti-static raised flooring with designated power runs and cooled air delivery
Network Operations Center (NOC)	• Three, mirrored Network Operations Center (NOC) • Staffed 24x7x365 by experienced engineers • Monitor both local and regional networks including POPs, telecom facilities, routers, servers, and customers' infrastructure including event notification and ticket tracking • Remote Hands capabilities available 24x7x365
Telecommunications Network	• Redundant fiber optic networks (All major Telecommunication providers) delivered via Bellcore standards with secure conduit and separate entrance facilities • Telecommunication services available from T1 to OC48 and Gigabit Ethernet
Data Redundancies	• Separate servers at different locations back up data through replication services. • Nightly hard copy backups created and transferred monthly to a secure location • DBA ensures a hot spare of all active databases, which can be put into use within minutes of the primary's failure. Secondary backups of vital data will be kept off-site and can be restored within 8 hours.

Software Security

Intrusion Detection	• 24x7x365 Detection of malicious activity • 24x7x365 Reporting and monitoring of all activity an all network access points • 24x7x365 Alert signature and system management • 24x7x365 Proactive protection through alert signature and system management • Regular reviews / audits of all user logs
Access Control	• Passwords stored using one-way encryption • No remote software is installed on Workstations • Secured login, passwords are encrypted, non-disclosure of full ID's on-screen, automated log-out. • Session activity is terminated when a security-related parameter has been exceeded or violated
Application Software	• Our servers run under the Linux operating system and use Apache Web Server, MySQL Database, and other solutions written in PHP, and JAVA. All applications are developed and designed first for security. • Audible and text alert systems are in place and triggered if any "critical issues" occur, such as when the site is inaccessible, or when an alternate power supply is activated. Monitoring system extends off-site to IT Administrator. List of “critical issues” can be provided upon request.
3rd party software	• Client-side browser. As an ASP model, updates are automatic and no additional 3rd party software is needed.
Testing Environment	• All new applications and extended features go through three levels of testing: 1) Application is tested on development machines by developers, 2) then handed off to testers who verify application functionality in an environment that mimics the end user environment, 3) and then the application is tested in a production environment with a panel of real-world users.
Authorizations	• Authentication is HTTPS SSL compliant. The client's web browsers needs to support 128-bit SSL encryption. • System can be extended to work with LDAP.
Change Control Management	• When an internal or external client identifies a needed change in the application, requests are evaluated by application support team for feasibility and effectiveness. Approved changes are coded in development environment, then tested and verified by test team. Changes are then implemented in the production environment and test team again verifies the change in production as well as performs regression tests. Support team then notifies interested parties of the effected change. (Minimum 4 week expectancy for all changes requested) • When necessary, all features can be modified and updated in real-time.

Demographics/Server Load	• Increased load would be handled by increased throttling techniques or eventually requesting more bandwidth from our Internet Service Provider. • Server machines can easily be added to accommodate the application load. • Some clients have dedicated machines for their service (including some or all of the following, dedicated database server, web server and/or other dedicated security measures • Qualtrics guarantees industry standard up time of 99% a year with no more than a total of 24 hours / year. This is detailed more extensively in the license agreement.
Portal Integration	• Qualtrics is currently capable of SSO authentication.
Load, Stress and Penetration Testing	• Apache bench utility and other in-house tools are currently used to conduct load, stress, and penetration testing. • Jan '07 results show that Qualtrics is capable of handling: mailings, minimum of 86,000 in a day; survey responses, Minimum of 1.2 million per day per web server.

Qualtrics Defines Data Security for its clients in 4 different areas:

Level 1 (Public) information is information that can be disclosed to anyone. The information is already in the public domain, approved for the public domain, and because it has already been made public, no one can claim a reasonable expectation that such information should remain private. Knowledge of this information does not expose the Firm to financial loss, embarrassment or jeopardize the security of Firm assets.

Level 2 (Business Confidential) information is typically required to perform normal day-to-day work and may be accessed by all Firm personnel. Internal Use Only information may be shared within the Firm, but must not be shared with consultants, vendors or temporary workers unless a non-disclosure agreement has been signed.

Level 3 (Restricted) information is information whose unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on the Firm, its customers, intermediaries or employees. Restricted information may be shared with parties who have a relationship with the Firm, if they have signed a non-disclosure agreement, and have a need to know.

Level 4 (Secret) information is characterized as sensitive information that is intended for a very limited group of individuals who must be specified by name. This level contains information, which if disclosed would provide access to business secrets and could jeopardize important interests or actions of the Firm or its clients and would be to the serious personal or financial detriment if revealed to unauthorized persons.

HIPAA Compliance

With the Health Insurance Portability and Accountability Act (HIPPA) Qualtrics understands that there are four distinct areas defined by the Department of Health and Human Services (DHHS):

1. Administrative procedures — Procedures for establishing and enforcing security policies
2. Physical safeguards — Safeguards that protect physical computer and network facilities
3. Technical security services — Services that protect, control, and monitor access to health care information
4. Technical security mechanisms — Mechanisms for protecting information and restricting access to data transmitted over networks

Qualtrics understand its responsibilities to include the following area only: Physical safeguards. Details about that Qualtrics compliance are found previously in this document. The other three areas are out of Qualtrics control and are the responsibility of the purchasing company to establish procedures and mechanisms that maintain and enforce appropriate security policies that comply with HIPAA.