APTS Data Security and Privacy

APTS is a certified vendor with the California Student Privacy Alliance as well as the Massachusetts Student Data Privacy Alliance.

Regulations

To enable delivery of services, APTS collects via the APTS Platform information including names, addresses, email and telephone number. Depending on the exam registration process level of complication, APTS may also need to collect additional subject specific information and student grade level such as with Advanced Placement and International Baccalaureate exams. APTS may also need to receive from the APTS Client Organizations information include name, email and student course enrollment.

All information collected shall be treated as "Protected and Confidential Data" (referred to henceforth as 'Data') and will be processed and handled according to the following regulations:

1. Data is collected via forms served over 256-bit SSL secure connection.
2. Data shall be stored on a secure remote server.
3. All data will be viewed and modified on the server over an encrypted network connection.
4. Data will be accessible to:
    a. APTS Staff: Staff will be able to log into the data server via a 128-bit encrypted connection along with a strong password strength.
    b. APTS Client Organizations: Client schools will be allowed log in access via a secure 128-bit encrypted connection portal. This portal access will provide the school designee (testing coordinator or administrator), 'view only' access to be able to complete their testing coordination but not modify any data.
    c. Individuals: Individuals who submit an exam order through APTS will be able to request in writing a copy of their registration data, including all pertinent logs. Requests must be submitted via email and must originate from an email address on file with APTS and connected to that specific individuals' order. Corrections to data that had been submitted to APTS can be requested in writing. The request must originate from an email address on file with APTS and connected to that specific individual. A confirmation will be issued by APTS once the data has been updated. Information will not be released at any time by phone and corrections or changes requested by phone will not be processed or accepted by APTS.
5. APTS will never collect social security numbers.

6. Data will NOT be shared or disclosed to any other organizations or institutions, non-APTS staff or non-client organization. This restriction applies to source data as well as all derived data files.
7. The data security protections apply to the original data, derived files, and temporary analysis files. Data fields such as student ID number will be encrypted and not searchable in the server nor included in any email notifications.
8. APTS Staff shall attend twice annual HIPAA and FERPA training to review State, Federal and local regulations, changes in regulations, and legal boundaries for data use, especially as it pertains to providing the APTS Client Organization with support resources as well as customer service support through the APTS toll free call center to individuals. Logs are retained of all data access, updates or changes made by APTS staff.
9. Credit card information will not be collected or stored on the data server. Credit card payment information will be collected and processed on a separate merchant gateway server with secure encryption that confirms to the Payment Card Industry Data Security Standards ("PCI-DSS") and Payment Application Data Security Standards ("PA-DSS.") The APTS merchant gateway server and all integrating applications must all be at all times PCI-Compliant. APTS Staff will be able to log into the merchant gateway to access credit card information elements only to the following extent: transaction ID, transaction amount, credit card type and transaction date. APTS will be able to process a refund back to the original transaction card ONLY. No credit card numbers are accessible at any time.

Technical Details

Data is collected via forms served over 256-bit SSL secure connection and stored on a secure remote server. The server is remote and off site to enable storage in a safe, secure environment. Server is located in a SOC 2, Type II audited facility that is located in the United States. The data center includes high-end surveillance equipment, security guards, visitor logs and passcards/biometric recognition. With fully redundant IP connections, independent connections to T1 access providers, redundant external and internal power supplies, daily security scans and encrypted offsite backups. The facility has disaster recover plans in place that includes offsite backups in the event the current data center is not accessible or inhabitable. Disaster recovery plans are reviewed frequently.

In case of anomalous behavior, the facility system administrator will automatically contact the APTS Staff designee with administrative rights. The APTS Staff designee with administrative rights can then determine whether to isolate data, close log in access to the Platform, or close the Platform to run system check or log review. Log files are kept on file for 6 months to enable review. In the event of a breach, affected APTS Client Organizations as well as affected individuals will receive notification via email within 24-

hours of detection. Notification will include a detail of affected data as well as recommended steps to ensure data safety.

The data server uses an outside routing layer that provides filtering to handle and manage any potential denial of service attacks. All network traffic then has to pass through redundant firewalls. APTS and the remote server storage facility performs frequent scans, including PCI scans by McAfee, to look for any potential vulnerabilities in the network. Access to the server for APTS Staff and Client Organization designees is via use of a 128-bit encrypted connection along with a strong password strength.

Timeline for Data Use and Retention

Data is under active security analysis and accessible to the APTS Staff and Client Organization for 90 days after the completion of the exam administration. Data is not retained or kept from year to year or exam to exam administration. Data will be deleted and destroyed from the server and no access would be possible by APTS or the APTS Client Organization 90 days after the completion of the exam administration. (For example, if the last day of AP exam administration is on May 24, 2020, the data will be scheduled for destruction 90 days after May 24, 2020.)

For more information, contact info@aptsusa.com

Revised and Updated: July 16, 2020