Apex Revenue Technologies: An Overview of Our Security Practices

WHITE PAPER – SUMMER 2017

Apex Revenue Technologies:
An Overview of Our Security Practices

WHITE PAPER – SUMMER 2017

As a healthcare provider or a business that supports healthcare clients, you have an obligation to safeguard patients' sensitive information—both health-related and financial. When you bring an outside partner into your business, it's imperative to choose one that takes patient privacy as seriously as you do.

Apex Revenue Technologies is that partner. Our facilities, infrastructure, services, technologies, employees, and vendors are managed to the highest levels of security, earning us multiple industry certifications as well as technology awards. As your business partner, we work to ensure the safety and security of the information we process. At Apex, information security isn't just a box to check off—it's woven into our corporate DNA.

In this paper, we've outlined how Apex provides security assurance in four key areas:

1. Corporate Facilities
2. Network and Platform
3. Financial Information
4. Patient Health Information

> *Our facilities, infrastructure, services, technologies, employees, and vendors are managed to the highest levels of security, earning us multiple industry certifications as well as technology awards.*

I. Corporate Facilities

Physical access to Apex's production facilities is restricted to authorized individuals by card-key systems. Upon entering the building, visitors are vetted and required to sign a log. Video surveillance and card-key tracking software are in place to monitor access. A review of employees who have access to the facility, systems and applications is conducted regularly.

Apex also uses two fully redundant Tier III data centers—separate from our production facilities and corporate network—to host, process, and store data. Our primary data center is a Type 2 SOC 2-compliant facility in Minneapolis, Minnesota. Redundant data services are also hosted at a Type 2 SOC 2-compliant data center in Nashville, TN. Physical access to data centers is restricted and guarded by security personnel and cameras.

II. Network and Platform Security

Network

Apex utilizes state-of-the-art Palo Alto firewall and IDS systems for network security, which includes protection against denial of service (DoS) attacks. Failed connection attempts and brute force attacks are logged. Firewall restrictions are in place to allow only certain Internet Protocols (IPs) into the hosting environment. Separate VLANs are in

place to restrict user and application access to the appropriate servers. Multi-layer perimeter security is also provided through firewalls between internet and web servers and web servers and application servers. All end points including workstations, laptops, and servers are protected by an antivirus/malware protection system that uses mathematical algorithms to identify and quarantine potential threats.

Apex utilizes state-of-the-art Palo Alto firewall and IDS systems for network security, which includes protection against denial of service (DoS) attacks.

Platform

Our systems run on hardened Windows servers with the latest security patches and virus protection installed. The system undergoes annual penetration tests and quarterly internal and external vulnerability scans. All identified vulnerabilities are remediated within 30 days. The system is monitored through a centralized monitoring systems that sends email alerts when suspicious activity or performance issues arise.

Apex provides mySecureBill® and myEasyView® services using a hosted model, designed expressly to ensure robust and secure operation. mySecureBill® and myEasyView® are patient payment and patient support portals that enable secure browser and smart phone access to statements, payment services, and account message and tracking information. These services are comprised of the following components:

Browser: The end user accesses the system through a web browser installed on a personal computer or mobile device. Users access the system by visiting an Apex-hosted website and entering a username and password, which is transmitted to a web server for authentication. Single sign-on (SSO) requests originating from provider applications are also supported. All traffic between browsers and application servers is encrypted via Secure Sockets Layer (SSL).

Web servers: All traffic originating from browsers is handled by hosted, load-balanced web servers that operate within a DMZ and communicate with application servers to process end-user requests.

Application servers: Application servers, data processing servers, and email servers are housed in a hosted and segmented application environment consisting of Windows-based servers.

File transfer: Clients using Apex messaging and billing services upload data files, such as statement, marketing, and other integration data, to our hosting facility for distribution to patient end-users.

All data is transmitted through secure, encrypted protocols including SFTP, FTP/S, and HTTP/S and immediately moved into the application environment for processing. Apex supports PGP encryption of uploaded data.

Data storage: All application data is stored in an encrypted database. Files transmitted to and from Apex are encrypted in transit and at rest. All client data is segmented within the database by unique customer identifiers. All databases and files are stored at our redundant Tier III datacenters.

Administration

Internal Administration Interface

Apex servers are administered over private VPN connections that require two-factor authentication. Remote Desktop Protocol (RDP) supports authenticated and encrypted remote log-in access by Apex authorized staff. Access to production servers is limited to authorized Apex personnel and access is granted by employee role. Workstations and laptops are configured to launch a password-protected screen after 15 minutes of inactivity to ensure that unattended systems are not vulnerable to unauthorized use.

All Apex workstations and laptops are encrypted and have endpoint antivirus/malware protection installed and operational.

End-User Administration Interface

Administration services are accessible from any web browser. Clients may opt to restrict access to the IP addresses originating from their corporate network. This interface provides access to patient user information, application configuration, and reports. All traffic between the administration interface and browsers is protected using SSL. Provider users authenticate their access to the administration website with a username and password that must be changed every 90 days.

Data available via the administration screens is limited to what is needed for provider users to manage their application. Sensitive end-user data may be masked so that it cannot be read by provider users.

Passwords

Our system has strong password requirements with specific length and character restraints and a visual indication of password strength. Patient passwords are only displayed to administration-level users in the case of a manual password reset. The password displayed is randomly generated and the recipient user must change the password upon next login.

Apex systems use a cookie to identify authenticated users that have logged in via a web browser. This cookie holds a unique ID generated at the time of access, and does not contain any personally identifiable information or passwords. It is only valid for the length of the user's browser session.

Client System Integration

Client practice management systems can be seamlessly integrated with Apex systems using single sign-on (SSO). This technology simplifies the navigation between multiple systems while maintaining a high level of security. To securely connect a client's system with Apex's myEasyView® or mySecureBill® portal, without requiring additional support representation or administration login, one or more access points can be defined and secure connections can be linked between systems.

III. Financial Information Security

Apex is certified by the PCI Security Standards Council as being fully PCI-DSS compliant. This certification is the result of a yearly assessment that confirms our company meets all twelve guidelines set forth by the organization. While PCI compliance alone is a differentiator, we go one step further to offer payment solutions that can reduce our clients' PCI compliance scope and liability. Our commitment to financial data security spans three critical areas where exposure can occur:

- POS (Point-of-Service) payments made on-site at a client's facility
- CSR (Customer Service Representative) payments made over the phone
- Online payments and phone payments made via IVR (Interactive Voice Response)

Apex's financial security measures include:

Point-to-point Encryption Technology. Apex's POS platform is fully P2PE- (Point-to-Point Encryption) compliant. P2PE is a payment card security solution that instantly translates cardholder data into indecipherable code at the moment of swiping, which in turn prevents data theft. For POS payments and phone transactions handled by CSRs, Apex clients use an external Point-of-Interaction device that allows users to swipe or key in financial card data. This device supports all payment types and allows for the processing of cardholder data apart from the staff member's workstation.

Even when it comes to online payments and credit card information spoken via IVR transactions, card data is never stored. Rather, it bypasses the client's network and is routed for authorization directly to CardConnect, the gateway service utilized by Apex that is fully P2PE-validated by PCI.

> *While PCI compliance alone is a differentiator, we go one step further to offer payment solutions that can reduce our clients' PCI compliance scope and liability.*

EMV Compliance. EMV involves the use of microchip-reading technology to shield consumers against the misuse of lost or stolen cards; it also makes credit card replication more difficult for identity thieves. Apex's myEasyView® POS platform is fully EMV-compliant. All POS payment transactions are processed through CardConnect, one of only a few gateway providers that are EMV-certified. Coupled with P2PE, EMV compliance helps to significantly strengthen cardholder security.

Apex Revenue Technologies is certified by the PCI Security Standards Council as being fully PCI-DSS compliant.

IV. Patient Health Information Security

At Apex, compliance is not a point in time; it is ongoing and integrated within our daily business activities. Since we serve more than 500 healthcare clients nationwide, all aspects of our business are structured with Health Insurance Portability and Accountability Act (HIPAA) compliance in mind:

- We have an **internal HIPAA Compliance Officer** who evaluates legislative and regulatory changes for impacts to our current processes, products, or services. This individual creates and/or modifies appropriate policies and procedures to address regulatory or operational changes. They also lead our annual Security Risk Analysis to ensure our security controls are protecting the confidentiality, integrity, and availability of the protected health information (PHI) we access, receive, create, store, modify, or transmit on behalf of our clients. In the event of a data breach, it is the duty of our HIPAA Compliance Officer to handle the incident in strict accordance with HIPAA regulations.
- Apex conducts **mandatory, annual compliance training** for all employees. Additionally, quarterly meetings are held with executive staff members to evaluate the state of our compliance, address new requirements, and make modifications as needed to policies, procedures, or processes.

System Integrity

The Apex infrastructure is both robust and secure. Redundant routers, switches, firewalls, servers, databases, and backup systems are used to ensure high availability during normal business operations. For scalability and reliability, incoming traffic is transparently distributed among Apex web servers. Web application servers are placed in a DMZ, separate from the internal network.

Apex clients enjoy peace of mind, thanks to our robust and highly stable infrastructure, which allows us to deliver 99.9% system uptime/availability. Comprehensive disaster recovery strategies ensure rapid data backup and restoration in the event of a disaster.

Business Continuity

Apex maintains stringent plans and procedures to ensure rapid data backup and restoration in the event of a disaster that results in our primary systems being down or unusable. Our Business Continuity/ Disaster Recovery Plan provides guidance and direction to ensure the safety of employees and the resumption of time-sensitive operations in the event of a disruption that may affect our ability to service our customers—or a disaster that may be terminal or devastating to one or more Apex print or data centers.

Our recovery plan covers our print and mail operations as well as our e-delivery products and services. We have established a formal Business Continuity/Disaster Recovery Team and key roles to ensure a smooth deployment in the event of a disruption or disaster. Lastly, Apex actively hosts activities throughout the year to maintain our Business Continuity / Disaster Recovery Plan and ensure the processes are defined accurately, staff members understand their role in the event of a disruption or disaster, and our plan remains current.

Internal Security Policies

Apex understands that privacy and data security are critical in delivering customer-facing service, which is why we maintain rigorous internal security plans, policies, and procedures.

- Apex has a **strict privacy policy** that prohibits unauthorized disclosure of personal or corporate information to any third party unless expressly authorized to do so. This includes certain user information that we must maintain while delivering our services such as first and last name, email address, account-level passwords, and often account numbers and other sensitive end-user data.

Apex has a strict privacy policy that prohibits unauthorized disclosure of personal or corporate information to any third party unless expressly authorized to do so.

- Each **new employee undergoes extensive screening**, which includes OIG exclusions and criminal background checks, prior to being offered employment.
- New employees undergo **security awareness training** within 30 days of employment.
- Upon **employee termination**, access to facilities, systems, and networks are discontinued, and all assets are collected immediately or prior to separation.

Apex: A Partner You Can Trust

Apex's approach to security is straightforward: Start with protected facilities; secure, hosted services; and operational practices designed to preserve provider and patient privacy. Complement this foundation with secure, enterprise-class configuration and monitoring tools to control remote access.

The result: robust, secure healthcare messaging and billing services with a low total cost to implement. You can feel confident working with Apex Revenue Technologies—a proactive, experienced partner who cares about protecting not only your interests, but also those of the patients who are the backbone of your organization.

Apex Revenue Technologies | 100 South Owasso Blvd. W. | Saint Paul, MN 55117 | P: 866.676.2739 | F: 651.287.8203 | info@apexrevtech.com

About Apex Revenue Technologies

Founded in 1995, Apex Revenue Technologies is a national provider of technology-based solutions and services to healthcare companies wanting to improve revenue cycle management. Our cloud-based software promotes patient financial engagement, protects patient data, streamlines billing processes, increases revenue, and reduces the cost to collect.

Start seeing results sooner than you can imagine. Set up a discovery meeting today.

To learn more, visit **apexrevtech.com**

APEX

Apex Revenue Technologies | 100 South Owasso Blvd. W. | Saint Paul, MN 55117 | P: 866.676.2739 | F: 651.287.8203 | info@apexrevtech.com