

NO BREACHES

NASCO has always been committed to protecting our customers' data, and with the widened scope of privacy and security protections available under HIPAA and the increases in enforcement and legal liability for non-compliance, we understand the increased importance of our commitment to system stability and security.

To ensure the highest level of data protection, NASCO has many controls in place for physical and network security. The NASCO Processing System's (NPS) physical location is secured with restricted access and equipped with magnetic and biometric entry systems and video surveillance. The data center that houses the NPS has backup power provisions in place to supply uninterrupted service for critical areas. In addition, NASCO ensures that all equipment is properly inspected and maintained. We also have a full disaster recovery plan, which is tested annually with our Plan customers.

The NPS operates within a private, closed, trusted network environment consistent with HIPAA standards. It is not accessible via the Internet; the only way to connect to the NPS is via BluesNet, and data transmissions are sent via approved, secure transmission protocols. The various processing networks within the NPS are controlled and restricted via switching technologies. In addition, firewalls have been strategically implemented to restrict unsolicited data traffic and services. We also perform quarterly intranet-based vulnerability scanning to assess our system's security configuration compliance.

In addition to the extensive measures we take to ensure NPS and network security, NASCO is also committed to ensuring that all our internal hardware meets the same security standards. All NASCO hardware is encrypted, which means that if any NASCO computer is lost or stolen, the data on that computer will remain protected. We also have special email security hardware that recognizes protected health information within emails and forces the delivery of such emails through a secure network connection or requires the recipient to authenticate to our secure network to access the email.

While we know how important the physical and network security of our system is, we also understand that security goes far beyond those controls. With a Certified Information Systems Security Professional as our privacy and security official, NASCO requires all our associates and vendors to complete the HIPAA Privacy Rules and Security Rules training on an annual basis. NASCO includes Privacy and Security Awareness training as part of our new-hire orientation for all associates and requires completion of an online assessment. We have also strengthened our HIPAA business associate agreements with all our vendors.

Securing our customers' data is the responsibility of all NASCO associates, contingent workers and business associates, and it is something that we all take very seriously.

