DELTA DENTAL®

Your Security is Our Top Priority

At Delta Dental of Michigan, Ohio, and Indiana, we take our responsibility to protect and safeguard your information very seriously.

Our strategy to secure personally identifiable information (PII), protected health information (PHI) and other forms of privacy information is multifaceted and includes:

Encrypting our data

Desktops, laptops and servers are encrypted where privacy data is stored; removable media such as thumb drives, CDs and DVDs are strictly limited to approved personnel, and all data written to those devices is encrypted; backup tapes containing privacy data are encrypted.

Securing our locations

Employees wear radio frequency identification (RFID) security badges to access buildings and interior secured areas on the main campus; internal and external video cameras are monitored 24 hours a day, 365 days a year.

Strictly governing passwords and access

Passwords are changed at regular intervals, and "strong" passwords are required; we review accounts regularly for appropriate access; access is immediately revoked on all employee terminations/separations; two-factor authentication is in place for all privileged users.

Conducting checks

We perform background checks on all employees and contractors prior to being granted access to systems.

Protecting our systems

Anti-virus is installed and updated on all desktops, laptops and servers; internal and external firewalls segregate internet-facing traffic from internal, and they segregate internal users from direct access to servers; Intrusion Prevention Systems (IPS) are installed at critical "choke points" on the network; egress filtering reduces the threat of command and control malware infections; email gateways identify and encrypt messages that contain privacy information.

Testing our security

We regularly try to penetrate and exploit our systems to make sure everything is functioning as it should and no weaknesses exist.

These safeguards and more comply with guidelines issued by The National Institute of Standards and Technology (NIST) 800-53 Special Publication on Recommended Security Controls for Federal Information Systems and Organizations, the Center for Internet Security (CIS) Benchmarks, and the Department of Defense (DoD) Security Technical Implementation Guides (STIG).