Delta Dental Plan of Michigan, Ohio, and Indiana

Information Security Policy

Procedure #:	435-24	**Title:**	Information Security Policy		
Issue Date:	10/17/2018	**Next Review Date:**	03/28/2024	**Last Review Date:**	3/28/2023	**Last Revised Date:**	3/28/2023
Owner:	Andrew Woodard, Vice President, Chief Information Security Officer	**Executive Sponsor:**	Mark Baughman, SVP & Chief Information Officer		
Reminder: When accessing PHI or other sensitive information, employees must at all times abide by the Company's Minimum Necessary Privacy Policy					

Table of Contents

Revision History

NAME	DATE	VERSION	SUMMARY OF CHANGES
Andrew Woodard, Meredith Sharp	04/18/2016	1.0	Initial Draft
Andrew Woodard, Meredith Sharp	07/11/2017	2.0	Annual review and risk assessment updates
Andrew Woodard	11/7/2017	2.1	Privacy Officer name change
Andrew Woodard	12/7/2017	2.2	DDPA updates
Andrew Woodard	03/19/2018	2.3	USB Use and Authorization
Andrew Woodard	03/18/2018	2.4	Privacy Officer name change
Andrew Woodard, Meredith Sharp, RHSC Security Council	10/17/2018	3.0	Revisions for RHSC Enterprise-wide Policy Updates
Andrew Woodard, Meredith Sharp, RHSC Security Council	01/15/2020	3.1	Annual review and revisions/updates; Privacy Officer name change
Andrew Woodard, Meredith Sharp, RHSC Security Council	2/11/21	4.0	Annual review and revisions/updates; additions for HITRUST compliance
Andrew Woodard, Meredith Sharp	February 11, 2022	5.0	Revisions for HITRUST compliance
Andrew Woodard, Meredith Sharp	March 28, 2023	5.1	Annual review and revisions/updates

Approval History

NAME	DATE	VERSION	SUMMARY OF CHANGES
Data Privacy Committee	04/18/2016	1.0	Initial Draft
Data Privacy Committee	07/11/2017	2.0	Annual review and risk assessment updates
Data Privacy Committee	12/14/2017	2.2	DDPA Updates
RHSC Executive Cybersecurity Committee	10/17/2018	3.0	Revisions for RHSC Enterprise-wide Policy Updates
RHSC Executive Cybersecurity Committee	01/15/2020	3.1	Annual Review and Updates
RHSC Executive Cybersecurity Committee	03/23/2021	4.0	Annual review and revisions/updates; additions for HITRUST compliance
Compliance Committee and Data Governance & Protection Committee	February 11, 2022	5.0	Revisions for HITRUST compliance
Compliance Committee and Data Governance & Protection Committee	March 28, 2023	5.1	Annual review and revisions/updates

1. Introduction

A. PURPOSE

Delta Dental Plan of Michigan, Ohio, and Indiana ("Delta Dental") is committed to protecting all RHSC Confidential Information relating to its clients, employees, and business operations. Delta Dental Strictly Confidential Information and Federal Government Confidential Information (as defined in Appendix B) must be protected by ensuring the appropriate level of security controls is applied and effective. These controls are designed to safeguard Delta Dental operations, protect Delta Dental's reputation, and enable Delta Dental to safely and securely deliver services to its clients.

This policy defines the technical, administrative and physical controls all Delta Dental users are required to implement in order to ensure the confidentiality, integrity and availability of the data environment at Delta Dental, as well as compliance with the HIPAA Security Rule, Payment Card Industry (PCI), customer requirements and applicable National Institute of Standards and Technology (NIST) controls. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides business owners, system owners and Data Owners within Delta Dental with policies and guidelines concerning the protection of Delta Dental data, technology equipment, Email, Internet connections, voicemail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to workstations, servers, containers, network infrastructures, cloud environments, mobile devices, databases, external media, Encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey data, knowledge and ideas across all hardware, software, and data transmission mechanisms.

B. SCOPE

This policy applies to anyone using or accessing the company's information systems and includes all employees, contractors, consultants, vendors, temporary staff, interns, and/or other workers at the company (sometimes referred to as "Personnel"). It also includes any guests who access the company's wireless networks or other IT assets. Further, it encompasses anyone who has knowledge of or access to proprietary or other sensitive company information or materials.

This policy encompasses all information systems equipment, including but not limited to computer equipment, software (proprietary or third-party), operating systems, disk storage media, servers, containers, network devices, cloud environments, user login accounts (computer, application), Internet browsing, FTP, telephones, cell phones, smart phones, tablets, photocopiers, scanners and fax machines. The use of the company's information systems and related equipment is for company business and for authorized purposes only in accordance with this policy.

In the event of a conflict with other policies, regulations or customer requirements, the more restrictive measures apply.

This policy is not intended to address employee responsibilities with respect to the HIPAA Privacy Rule. Please refer to company Privacy Policies.

C. APPLICABLE STATUTES / REGULATIONS / STANDARDS

The following is a list of the various agencies/organizations whose laws, mandates, regulations and standards were incorporated into the various policy statements included in this document.

- Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules (45 CFR Parts 160 and 164)
- Other applicable Federal and State laws and regulations, including, but not limited to:
    - 201 CMR 17.00 et seq. (Massachusetts)
    - 23 NYCRR 500 (New York)
    - MCL 500.550 et seq (Michigan)
    - ORC Chapter 3965 (Ohio)
    - IN ST 27-2-27-1 through 27-2-27-32 (Indiana)
    - NAIC Insurance Data Security Model Law (Model Act being adopted in numerous states)
- National Institute of Standards and Technology (NIST) Special Publication 800 series. NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
- Payment Card Industry (PCI) Data Security Standard
- Center for Internet Security (CIS) Critical Security Controls
- HITRUST® CSF v9.3 Risk-based, 2-year (r) certification

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

D. INFORMATION ACCESS MANAGEMENT

Delta Dental has formal processes and procedures in place to authorize access to Confidential Information and systems. Please refer to the Delta Dental Access Management Policy for further detail.

1. Prohibited Activities

Personnel are prohibited from doing the following. This list is not exhaustive. Other prohibited activities are referenced elsewhere in this document, as well as the Employee Handbook (or entity equivalent), and the Acceptable Use Policy. Management approves the use of Delta Dental information assets and will take appropriate action (including sanctions) when unauthorized activity occurs. Such sanctions may range from formal discussions with the individual's manager to immediate termination. See the Acceptable Use Policy for further detail. If an incident occurs, Employees are expected to cooperate with federal or state investigations or disciplinary proceedings. Failure to do so will result in disciplinary action.

Crashing an information system - Deliberately crashing an information system is strictly prohibited. A user may not realize that they have caused a system crash, but if the crash occurs as a result of user action, or the user repeatedly performs an activity which is known to severely impact that system, the user may be subject to sanctions.

Attempting to break into an information resource or to bypass a security feature - This includes running password-cracking programs or sniffer programs and attempting to circumvent file or other resource permissions.

Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.

> **Exception - Authorized information system support personnel, or others authorized by the Enterprise CISO or the Local Security Officer/CISO, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.*

Browsing - Willful, unauthorized access or inspection of Delta Dental Confidential Information by users who have not been approved on a "need to know" basis is prohibited. Delta Dental has access to patient or subscriber level health information, which is subject to HIPAA requirements that a user must have a "need to know" before approval is granted to view the information. A purposeful attempt to look at or access information to which access has not been appropriately granted is strictly against company policy.

Personal or Unauthorized Software - Use of personal software is prohibited. All software installed on Delta Dental computers must be approved by the Enterprise CISO or the Local Security Officer/CISO.

Software Use - Violating or attempting to violate the terms of use or license agreement of any software product used by Delta Dental is strictly prohibited.

System Use - Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of Delta Dental is strictly prohibited.

Home Use of Delta Dental Corporate Assets - Only computer hardware and software owned by or approved by Delta Dental may connect to Delta Dental's network. Only software that has been approved for corporate use by Delta Dental may be installed on Delta Dental equipment. Delta Dental supplied computers or equipment are to be used in compliance with the Employee Handbook and Acceptable Use Policy. Personnel must read and understand the list of prohibited activities that are outlined herein. Modifications or configuration changes are not permitted on computers supplied by Delta Dental.

Storing Confidential Information in a Prohibited Location - Delta Dental users shall only store Confidential Information in appropriate, specifically defined locations on Delta Dental networks. Delta Dental shall implement and employ technical means to ensure that Confidential Information is stored only in these locations.

2. Electronic Communication, Email, Internet Usage

Delta Dental encourages the business use of electronic communications as a productivity enhancement tool, in compliance with the Employee Handbook and Acceptable Use Policy. However, all electronic communication systems and all messages generated on or handled by Delta Dental owned or approved equipment are considered the property of Delta Dental – not the individual user. Consequently, this policy applies to all Delta Dental employees and contractors, and covers all electronic communications including, but not limited to, telephones, cellular phones (smartphones), Email, voicemail, instant messaging, Internet, fax, workstations, and servers.

Delta Dental provided resources, such as individual computer workstations or laptops, computer systems, networks, cellular phones (smartphones), tablet computers, Email, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1. it does not consume more than a trivial amount of employee time or resources,
2. it does not interfere with staff productivity,
3. it does not preempt any business activity,
4. it does not fall under any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Delta Dental information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Delta Dental information resources for personal or commercial profit is strictly prohibited.
    d) Junk Email - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the email message immediately. Do not forward the email message to anyone.

Delta Dental is responsible for servicing and protecting Delta Dental's equipment, networks, customers, Delta Dental Confidential Information, and resource availability, and therefore is required to access and/or monitor electronic communications from time to time. Several different methods are employed to monitor activity on Delta Dental's systems, network, and other assets.

Delta Dental reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations, as well as Delta Dental policies.

Employees should structure all electronic communication with the understanding that the content may be monitored, and that any electronic communication could potentially be forwarded, intercepted, printed or stored by others.

3. <u>Internet Access</u>

Internet access is provided for Delta Dental users and is considered a valuable corporate resource. This resource impacts company expenses and encompasses inherent security risks. The Internet access provided by Delta Dental, and its use thereof, is subject to the Employee Handbook (or entity equivalent), and the Acceptable Use Policy. Excessive Internet use (e.g., streaming videos, music) may consume disproportionate bandwidth, which may negatively impact other users' abilities to perform daily job functions. Misuse of this resource, such as accessing non-business-related sites (e.g., shopping, social media, music sharing, etc.), may inadvertently introduce viruses or malware into the environment.

Individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time, consuming large amounts of bandwidth, or accessing inappropriate sites for personal use, disciplinary action may be taken.

Many Internet sites, such as peer-to-peer file sharing applications, chat rooms, streaming media, adult websites, and on-line music sharing applications, have already been blocked by Delta Dental. This list is constantly monitored and updated.

4. Report Software Malfunctions

TAC should be notified when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager, suspects a computer virus infection, the Incident Response Plan, or entity equivalent, should be followed, and the user must:

- Immediately stop using the computer.
- Not carry out any commands, including commands to <Save> data.
- Not close any of the computer's windows or programs.
- Not turn off the computer or peripheral devices.
- Physically disconnect the computer from networks to which it is attached (if possible).
- Inform TAC as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when it was first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Not attempt to remove a suspected virus.

5. Transfer of Confidential Information

When Confidential Information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of Confidential Information maintained by Delta Dental and hold all data in the strictest confidence. Any purposeful release of data or Confidential Information, to which an employee may have access, is a violation of Delta Dental Information Security Policy and Delta Dental entity Privacy Policies and will result in sanctions and possible legal action. In addition, output from applications handling Sensitive or Confidential Information will only be sent to users that are authorized to access the information.

6. Transferring Software and Files between Home and Work

Personal or Unauthorized Software shall not be used on Delta Dental computers or networks. If there is a need for specific software, submit a request to your manager. Users shall not use Delta Dental-purchased software on any non-Delta Dental computers or equipment, without prior written approval.

It is critical for Delta Dental to protect all Confidential Information; to do that effectively, Delta Dental must control the systems in which it is contained. Therefore, Delta Dental Confidential Information

shall not be placed on any computer that is not the property of Delta Dental without written approval from the CISO. In the event that a manager receives a request from a staff member, to transfer Delta Dental data to a non-Delta Dental Computer System, the manager shall obtain written approval from the CISO, prior to performing such a transfer of data.

Examples of Transferring Data to non-Delta Dental equipment:

- Copying email or email attachments to personal computers, tablets or smartphones.
- Forwarding Delta Dental email or attachments to personal email accounts (e.g., Gmail, Yahoo Mail, Hotmail, etc.).
- Copying work-related files to personal computers via VPN, Citrix, or File Sharing Tools (e.g., Box, DropBox, SkyDrive, SharePoint, etc.).
- Copying work-related files from portable devices (e.g., USB drives, flash drives) to personal computers, tablets, or smartphones.

The Delta Dental network is maintained with a wide array of security protections, which include virus protection, data loss prevention, Encryption of data at rest and in transit, Email file type restrictions, firewalls, intrusion detection and prevention hardware and software, etc. Since Delta Dental does not have jurisdiction over security controls on non-Delta Dental personal computers, Delta Dental cannot verify such controls are present on personal devices to protect Delta Dental Confidential Information.

7. Internet Considerations

Special precautions are required to block Internet (public) access to Delta Dental information resources not intended for a public audience, and to protect Delta Dental Confidential Information when transmitted over the Internet.

The following requirements shall govern Internet usage.

- Users shall not install or download any software (applications, screen savers, web browser toolbars, etc.). If users have a need for additional software, the user must contact their manager to submit a TAC service request;
- Confidential Information shall be Encrypted before being transmitted over the Internet;
- The Encryption software used, and the specific Encryption keys (e.g., passwords, passphrases), shall be approved by the CISO and meet minimum Encryption requirements defined within this document. The use of unapproved Encryption software and keys is prohibited.

Approval from the CISO shall be obtained before:

- Any Internet, or other external network connection, is established;
- Delta Dental Confidential Information is made available on any Internet-accessible computer (e.g., web or FTP server) or device;

8. Email Considerations

Special precautions are required to protect Delta Dental Confidential Information when transmitted via Email. Every Email must be inspected for malicious content for both incoming and outgoing Emails by an up-to-date, centrally managed product.

The following requirements shall govern email usage:

- While exchanging internal Emails containing Confidential Information with other Delta Dental staff, labels shall be placed in the "Subject" line stating, "Contains PHI". This is a warning to recipients of the Email, that the contents should be restricted to authorized personnel only.
- For Email that must be transmitted over the Internet and/or outside of the RHSC network, users shall not send Delta Dental Strictly Confidential Information or Federal Government Confidential Information via Email unless it is secured via Encryption;
- Users shall not use personal or other non-Delta Dental Email accounts (e.g., Yahoo, Gmail, Hotmail) to send Delta Dental Confidential Information;
- It is recommended users utilize Encryption to secure Emails containing Delta Dental Confidential Information, when practical.

The following are approved Email Encryption solutions:

- Proofpoint – This software is part of our Email infrastructure, in which users type the term "[Encrypt]" in the subject line of the Email to force Encryption of the Email, prior to being transmitted. If users attempt to send Email that may contain Delta Dental Confidential Information or Federal Government Confidential Information, the Proofpoint Data Loss Prevention (DLP) solution will block the Email from sending, until the keyword "[Encrypt]" is included.
- Microsoft Outlook – when drafting emails, if a user indicates that the message content is labeled "Strict" or "Federal"
- WinZip – Users may be required to use WinZip in the event the file size is too large, or the email recipient is not able to open the Proofpoint email. When Encrypting a file with WinZip, users are required to select the highest level of Encryption (e.g., AES 256-bit Encryption) and enter in a passphrase or password to protect the file. Further, users may not send the passphrase via Email. Users must contact the recipient via another communication medium (e.g., phone, fax, text), to exchange the passphrase. It is common to send the Email, then call the email recipient to provide them with the passphrase.

- • Other approved methods include:
  - Company Microsoft Office 365 Email Encryption
  - • Company Microsoft Office 365 Forced TLS configurations with specific entities, such as groups.

Approval from the CISO shall be obtained before:

Using any other solution to Encrypt an Email, including a customer or partner secure Email solution.

9. <u>Postal Mail and Courier Considerations</u>

Special precautions are required when sending ID cards, documents and portable media containing Strictly Confidential Information and Federal Government Confidential Information.

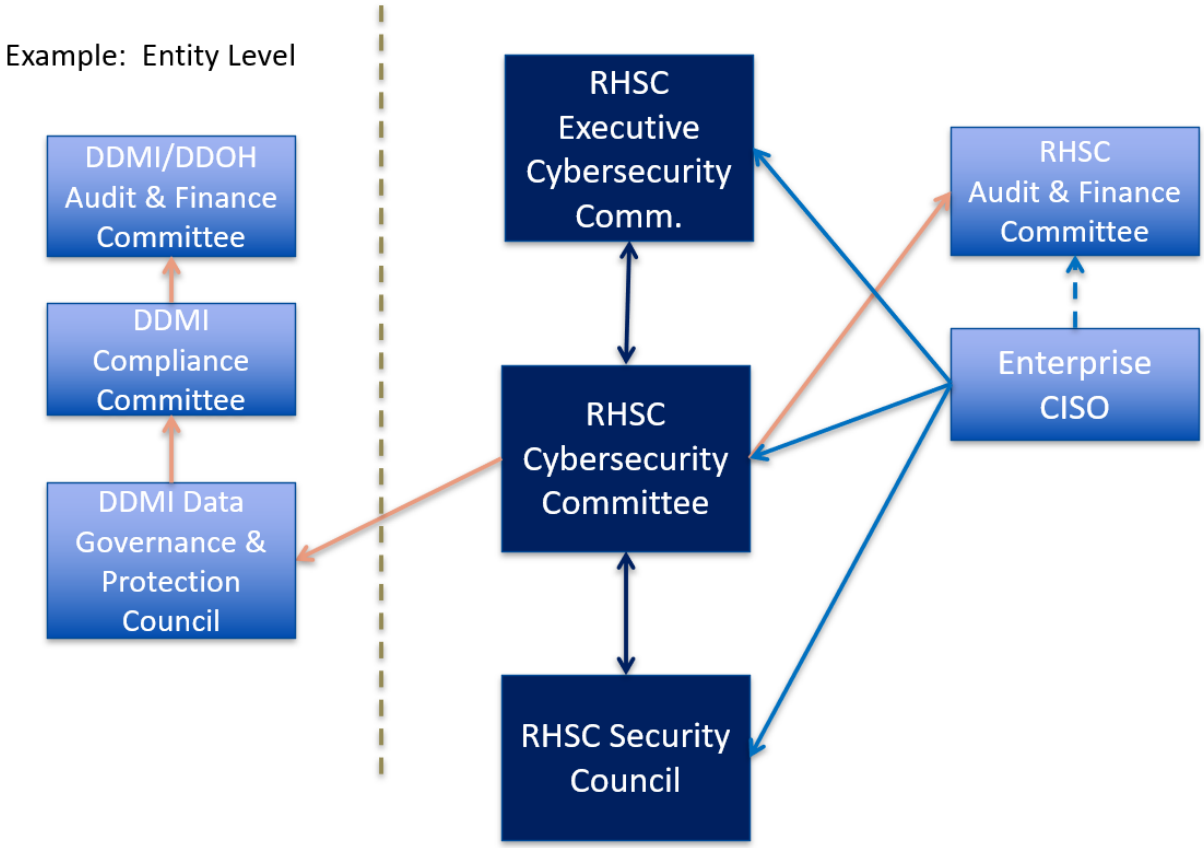
- Postal Mail – Must be sent first class or standard mail with endorsement, which includes return address service, in the event mail is sent to the incorrect address, postage prepaid for return back to Delta Dental.
    - Strictly Confidential Information and Federal Government Confidential Information must not be visible through envelopes and should be marked according to classification level
- Courier Mail – Must include tracking, including a representative of the receiving company, to sign upon receipt.

When sending portable media (e.g., USB or flash drives), the password or hardware key to decrypt the Confidential Information, must be sent separately. If a password is used, it the password must be sent via a separate channel. Therefore, if the portable media is sent via courier, the password should be either Emailed, faxed or communicated to the recipient via phone. The password cannot be sent within the same package as the media, ensuring the Confidential Information is protected in the event it is lost or stolen.

2. Administrative Safeguards

A. PRIVACY AND SECURITY PERSONNEL

Cybersecurity for the RHSC enterprise is led by the Enterprise Chief Information Security Officer (CISO). The Cybersecurity Governance model is as follows:



Enterprise CISO

- Leads improvement of overall security posture
- Leads policy, standard and process calibration
- Leads internal and third-party enterprise assessment (e.g., network penetration testing, compromise, HIPAA, PCI)
- Performs annual enterprise risk assessment
- Monitors risk assessment and third-party testing remediation
- Monitors enterprise cybersecurity risks and compliance

- NIST Cyber Security Framework (includes incident response readiness)
- HIPAA, PCI

- Keeps executive leadership and board informed – (e.g., dashboard)

  - Enterprise Risk Management (ERM), framework, enterprise risk assessment, third party testing (NPT, Compromise)

- Provides operational services and support where engaged
- Drafts policies at RHSC-level

Local Security Officers / CISOs

- Remain responsible for the security of systems and data hosted locally
- Participate in the Cybersecurity Council to help ensure cybersecurity threats, risks and any potential compliance issues are raised, discussed and appropriately shared with the Cybersecurity Committee
- Ensure respective security programs are in compliance with the Enterprise security policies and cybersecurity program
- Periodically report cybersecurity risks to the RHSC Enterprise CISO

RHSC Executive Cybersecurity Committee

- Approves strategic direction and policies
- Provides oversight

RHSC Cybersecurity Committee

- Chaired by Enterprise CISO
- Provides organizational guidance for current security issues or concerns across entities
- Assists in aligning security objectives with business objectives
- Advocates for security compliance and secure processes across entities

Entity Governance Bodies

- Approve strategic direction and policies at entity level

RHSC Security Council

- Chaired by Enterprise CISO
- Reviews, updates and enforces security policies for respective entities
- Ensures risk assessment and third-party testing remediation
- Communicates and discusses relevant projects

Each entity of RHSC has designated a Privacy Officer and a Security Officer with overall responsibility for the development and implementation of policies and awareness training that complies with applicable privacy and security laws. The Privacy and Security Officers shall provide customers and the public access to information about the entity's security and privacy activities, as well as a public-facing method for communication. The Privacy and Security Officers shall respond in a timely manner to any communications submitted using these methods.

Tristate, Renaissance (RLHICA, Ren NY), Delta Dental of North Carolina and Delta Dental of New Mexico:

- Privacy Officer: Meredith Sharp, Assistant General Counsel II & Privacy Officer
- Security Officer: Andrew Woodard, Vice President and Chief Information Security Officer (CISO)

Delta Dental of Arkansas:

- Privacy Officer: Katie Mehdizadegan, Vice President & General Counsel
- Security Officer: Mike Stephens, Director IT Solutions Center & CISO

Delta Dental of Kentucky:

- Privacy Officer: Danielle Jackson, Corporate Counsel
- Security Officer: Chris Green, Vice President, CFO

Delta Dental of Tennessee:

- Privacy Officer: Melissa Huschke, Chief Operating Officer
- Security Officer: Larry Hogg, Vice President, IS

The roles and responsibilities of the Local Security Officers/entity-level CISOs include:

- The individual responsible for information security in the organization (enterprise and local), must be qualified for the role.
- Establishing and maintaining a company-wide information security program ensuring that assets are adequately protected.
- Overseeing the development and communication of security policies and procedures.
- Along with the Privacy Officer, conducting risk assessments and implementing specialized workforce privacy and security education and training programs.
- Implementing additional specialized supplemental education and training programs appropriate for certain employees' roles/responsibilities, such as organizational business unit security POCs and system or software developers (see also Section 4F PATCH AND VULNERABILITY MANAGEMENT).
- Ensuring periodic security evaluations and continuous monitoring of Information Systems and Confidential Data.
- Identifying, evaluating and reporting on information security risks in a manner that meets compliance and regulatory requirements, and supports the risk posture of the enterprise.
- Providing leadership and vision to implement sound business management and information security technologies.
- Proactively works with business units to implement practices that meet defined policies and standards for information security.
- Conducting all assurance activities related to the availability, integrity and confidentiality of customer, business partner, employee and business information in compliance with these information security policies.
- Ensuring that information systems are maintained in a fully functional, secure mode in support of business needs.
- Participating as a member of the ISS Leadership or local information Technology Team, representing technology interests.

- Providing strategic risk guidance for IT projects, including evaluation and recommendation of technical controls.
- Working with the architecture team to ensure alignment between the security and enterprise architectures.
- Developing and implementing security requirements and standards for the acquisition of services and technology.
- Defining and facilitating the information security risk assessment process, including reporting and oversight of remediation of any identified findings.
- Managing information security incidents and events to protect IT assets, intellectual property, regulated data and the company's reputation.
- Monitoring for emerging industry threats and advising relevant stakeholders on the appropriate courses of action.
- Directing IT security purchasing and investments.
- Overseeing effectiveness of backup and disaster recovery policies, procedures and standards to align with enterprise business continuity management program goals.
- Coordinating the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of an information security incident. Providing additional direction, support and internal consulting in these areas.

B. PRIVACY / COMPLIANCE COMMITTEES

Each entity of RHSC has established a Data Governance & Protection Council (or equivalent governance body) to provide data privacy and security governance. The Delta Dental Data Governance & Protection Council is co-chaired by the Privacy and Security Officers (along with the lead of the Data Governance Office) and is made up of key personnel whose responsibility it is to identify areas of concern within Delta Dental and aid in the development of the appropriate security posture and policies for the company.

Data Governance & Protection Council members are identified by executive leadership encompassing all appropriate departments. The departments may include: Legal & Compliance, Accounting and Finance, Actuarial, Human Resources, Internal Audit, Risk Management, Customer Service, Group Administration, ISS/IT, Operations, Professional Services, Sales and Account Management, Culture, Communication & Community Affairs, and Actuarial/Underwriting.

The Data Governance & Protection Council roles and responsibilities include:

- Providing organizational guidance to the Privacy and Security Officers for current privacy and security issues or concerns within departmental areas
- Assisting in aligning privacy and security objectives with business objectives
- Discussing current privacy, security and risk issues, including action items and status
- Reviewing and approving proposed privacy and security policies
- Reviewing Internal and External Risk Assessment / Audit Results and assisting with the prioritization of any mitigation as required
- Attending Quarterly Meetings
- Advocating for privacy and security compliance and secure processes in respective departments and throughout the company

C. SECURITY MANAGEMENT PROCESS

Delta Dental recognizes that security policies, procedures, and controls must be reviewed and updated regularly by conducting accurate and thorough assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of Delta Dental Confidential Information. Delta Dental security policies, procedures, and controls must be implemented and maintained to prevent, detect, contain, and correct security violations.

As a result, the following processes must be in place:

1. IT Asset Lifecycle Program

- An IT Asset Lifecycle Program shall be implemented, monitored, annually reviewed, and updated, to ensure it effectively addresses the following six stages:

  (i) planning: defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts

  (ii) procurement: requisitioning, approving requisitions, ordering, receiving, and validating orders

  (iii) deployment: tagging assets, entering asset information in a repository, configuring and installing assets including: (a) disabling unnecessary or insecure services or protocols, (b) limiting servers to one primary function, and (c) defining: system security parameters to prevent misuse

  (iv) management: inventory/counting, monitoring usage (some software), managing contracts for maintenance and support, and monitoring age and configuration

  (v) support: adding and changing configurations, repairing devices, and relocating equipment and software

  (vi) disposition: removing assets from service, deleting storage contents, disassembling components for reuse, surplus equipment, terminating contracts, disposing of equipment, and removing asset from active inventory.

2. Inventory Information Systems

An inventory of all approved Information Systems, network equipment, wireless network equipment, portable media including laptops, hardware and software, that process, store, transmit, or access Confidential Information must be maintained and de-duplicated in an asset management system, which is reviewed and reconciled annually (365 days). Owners and custodians must be identified for all assets. Assets containing PHI/PII are identified within the asset inventory and provided to the CIO annually.

3. Inventory Confidential Information Data Sets

An inventory of all Confidential Information data sets must be identified and maintained and reviewed annually. The documentation must include the detailed information regarding the data set including the name, description, classification/criticality of data (e.g., PHI, PII), lifecycle, location, Data Owner, and custodianship.

4. Conduct Risk Assessments

Delta Dental must conduct an annual risk assessment that includes an accurate and thorough risk analysis of potential threats that may impact the Confidentiality, Integrity or Availability (CIA) of Delta Dental data or systems. The risk assessment analysis shall also include Delta Dental's HIPAA Security Rule compliance efforts, as well as compliance with other applicable laws, regulations, controls and standards, including (but not limited to) NIST 800-66 An Introductory Resource Guide to Implementing the HIPAA Security Rule, NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, NIST Cybersecurity Framework, Center for Internet Security (CIS) Critical Security Controls, HITRUST CSF**,** and Payment Card Industry Data Security Standard (PCI DSS), where applicable. The risk assessment encompasses technical, physical and administrative safeguards. It should re-assess security risks to the Confidential Information it processes, stores, transmits and accesses. It must also evaluate the effectiveness of its security measures, safeguards and controls as necessary in response to changes in business practices and technological advancements, vulnerabilities and threats, including a cost/benefit analysis for identified countermeasures. Delta Dental must have an independent audit conducted at least annually. Findings from this audit must be reviewed by management and corrective actions defined to improve security safeguards.

Delta Dental must conduct an annual HIPAA risk assessment. Risk assessments shall also be conducted whenever there is a significant change in the environment, or a change that could have a significant organizational impact. Depending on the scope of the annual enterprise risk assessment, the HIPAA Privacy Rule may not be captured within the scope. Delta Dental Each entity must also document all risk assessment and risk analysis artifacts.

Risk assessments may be performed by either internal or external personnel, with sufficient experience and knowledge to adequately perform the assessment. Risk assessments must be documented, including the controls assessed, deficiencies identified, and remediation status. Remediation must be completed in a timeframe commensurate with the severity of the risks identified.

Such risk assessments roll up into the Enterprise Risk Management (ERM) process. Because Delta Dental is a Member Company of the Delta Dental Plans Association (DDPA), any findings that are rated "high risk" (or greater), that:

- may take more than six (6) months to remediate; or
- cannot be mitigated; or
- is determined to be an "acceptable risk"

must be communicated to the DDPA CISO and DDPA CEO within seven (7) calendar days of such determination.

External risk assessments shall be conducted annually (or whenever there is a material change to business practices that may implicate the security or integrity of records containing personal information) in the form of a SOC 2. A SOC 2 provides an independent review of the organization's information security management program to ensure the continuing suitability, adequacy, and effectiveness of Delta Dental's approach to managing information security. The results of the SOC 2 shall be recorded and reported to the CISO and Director of Internal Audit and shall be maintained for at least three years. If the SOC 2 identifies inadequacies in the organization's approach and implementation to managing information security, or noncompliance with terms in the company's information security policies, management shall take corrective actions.

5. Security Assessment Upon System or Service Acquisition

Delta Dental's Security Officer shall ensure all IT systems, applications, and services that may relate to the processing, storage, transmission, or accessing of Delta Dental Confidential Information are evaluated for compliance with Delta Dental security policies, requirements, and applicable laws and regulations.

For any requests for access to security systems, the Security Policy Procedure Standard Variance Request Process must be followed.

6. Policy Reviews and Updates

Delta Dental security policies and procedures must be reviewed at least annually and updated accordingly. Any updates must be approved by the Data Governance & Protection Council, the TriState Compliance Committee, and the Board of Directors. Updates must also be communicated to all Delta Dental employees and contractors. Such communication may include Email, corporate Intranet sites, and training.

7. Reports to the Board of Directors

Annual cybersecurity program reports shall be made in writing to Delta Dental's Board of Directors and include, but not be limited to, the following:

- the confidentiality of nonpublic information and the integrity and security of Delta Dental's information systems;
- Delta Dental's cybersecurity policies and procedures;
- material cybersecurity risks to Delta Dental;
- overall effectiveness of Delta Dental's cybersecurity program;
- material cybersecurity events involving Delta Dental during the time period addressed by the report

8. Capital Planning and Investment

Capital planning and investment requests include the resources needed to implement the security program, employ a business case; and Delta Dental ensures the resources are available for expenditure as planned.

9. Internal Audits

Delta Dental's Corporate Audit and Advisory Services (Internal Audit) department shall perform an annual assessment of independently selected controls consistent with the internal audit plan as approved by the Board of Directors. The assessor should be independent of a control owner.

D. WORKFORCE SECURITY

Delta Dental shall restrict access to Confidential Information to the appropriate staff members. Delta Dental shall prohibit any other staff members from unauthorized access to Confidential Information.

Risk designations shall be assigned for all positions within Delta Dental and reviewed and revised annually. Additionally, the pre-employment process shall be reviewed by Human Resources to ensure security roles and responsibilities have been formally documented in all job descriptions, and that security roles and responsibilities are described to a job candidate prior to acceptance of an offer.

Delta Dental shall have additional policies and procedures captured in the Delta Dental Access Management Policy. The areas addressed from this section shall include, but are not limited to:

- Minimum Necessary Access
- Separation of Duties
- Software Development Access to Production Systems and Data
- Staff New Hire, Transfers and Terminations

The following workforce onboarding processes and activities shall also be in place:

1. Confidentiality agreements

All Delta Dental employees and contractors shall sign, as a condition of employment, a confidentiality agreement, acknowledging their understanding of their obligations and commitment to guarding information and data, and confirming that they will not disclose such information without the proper authorization.

2. Background checks

All employees and contractors must have background checks conducted prior to gaining access to Confidential Information. Subcontractor agreements shall require background checks in the event Delta Dental is not able to perform the required background checks.

As determined by Human Resources in compliance with all applicable laws, regulations and customer agreements:

- Candidates are qualified for the specific positions, based on the job description.

- Determinations are performed to ensure candidates are able to perform the tasks associated with the positions.
- Background checks may include any or all of the following: drug screening, employment verification, educational credentials verification, professional licensure verification, criminal record searches, civil record searches, driving record, credit profile, and Social Security Number trace.

E. SECURITY AWARENESS AND TRAINING

All Delta Dental employees and contractors, including senior executives, shall undergo privacy and security training as a new hire, as well as receive annual trainings. The training shall address core applicable regulations, standards and industry current events to ensure staff are knowledgeable on the proper handling and protection of Delta Dental Confidential Information.

The privacy and security (including HIPAA) awareness training must be completed within one week of the staff member's start date. Failure for the staff member to complete the training may result in the user's logical access/Logon ID to Delta Dental systems being disabled, until the training is completed.

In addition to privacy and security training programs delivered to all staff, information security and other ISS employees and contractors (depending upon their role) shall receive specialized role-based training upon hire, as well as annually. (See also Section 4F, PATCH AND VULNERABILITY MANAGEMENT)

Certain individuals who are named as representatives of the organization's cyber crisis management team (CCMT), or other equivalent incident response team, shall receive additional entity-specific awareness training regarding cyber crisis management as part of their roles and responsibilities. This will involve representatives from different departments within the organization, including (but not limited to) Information Security, Legal, and Human Resources, and shall include guidance on insider threats, in addition to external threats. Testing exercises shall be planned, coordinated, executed, and documented periodically, at least annually, using reviews, analyses, and simulations to determine incident response effectiveness.

Training shall be delivered utilizing appropriate and effective methods, including (but not limited to) computer-based Learning Management System (LMS) distribution; commercially available training modules; PowerPoint slide decks with custom content; in-person sessions; or other entity-approved methods. Upon completion of training programs (minimally new hire and annual refresher training), learners shall certify acceptance and acknowledgement of their security and privacy responsibilities.

Training programs, including a list of each employee or contractor who has undergone the onboarding and annual training, and the employee's or contractor's acknowledgement and acceptance of security and privacy responsibilities, shall be tracked and retained by the Compliance department in accordance with the requirements of Delta Dental's Mandatory Onboarding Training Policy and/or Mandatory Annual Training Policy (or other equivalent procedure), but for a period not less than five years.

Where practical, awareness training shall include quizzes. Quarterly phishing tests shall be performed as well.

1. <u>Security Training Program</u>

a) The Security Officer and Privacy Officer shall have responsibility for the development and delivery of the privacy and security awareness training. All workforce members, including senior executives, shall receive such training addressing the requirements of the HIPAA Security Rule

and Privacy Rule, including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act and the American Recovery and Reinvestment Act (ARRA). Attendance and/or participation in such training is mandatory for all workforce members. The CISO and Privacy Officer shall ensure appropriate documentation of all training activities is maintained. The CISO and Privacy Officer shall assess, at least once annually, the effectiveness of such training programs and make any needed program updates to reflect risks identified in the entity's risk assessment.

b) The HIPAA Security Officer and Privacy Officer shall have responsibility for the development and delivery of ongoing security and privacy training provided to workforce members in response to environmental, operational and industry changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats.

c) The HIPAA Security Officer and Privacy Officer shall have responsibility for the development and delivery of ongoing security and privacy training provided to workforce members which addresses topics including, but not limited to:

1. Mobile security
2. Telework
3. Appropriate organization-specified locations to store sensitive data
4. Industry principles and best practices for data handling in all types of information exchange (oral, paper, or electronic)
5. Mobile Device Management and Bring Your Own Device (BYOD), specifically
    a. Approved lists of applications
    b. Application stores
    c. Application extensions and plugins
6. Insider threats, including
    a. Reporting, in conjunction with the obligations of existing entity Fraud, Waste, and Abuse (FWA) and Code of Ethics and Conduct policies, of suspicious activity involving individuals accessing systems or viewing data that they should not be authorized to access or view

All training programs shall be distributed as described above, and in accordance with the Mandatory Onboarding Training and Mandatory Annual Training Procedures.

2. Security Reminders

a) The CISO shall generate and distribute routine security reminders to all workforce members. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The CISO may provide such reminders through formal training, Email messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The CISO shall be responsible for maintaining appropriate documentation of all periodic security reminders.

b) The CISO shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

3. Protection from Malicious Software

a) provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:

- Guidance on opening suspicious Email attachments, Email from unfamiliar senders, and hoax Emails,
- The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
- Instructions to never download files from unknown or suspicious sources,
- Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
- The importance of keeping data in a safe place,
- Damage caused by viruses and worms, and
- What to do if a virus or worm is detected.

4. Password Management

a) The CISO shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following policies relating to passwords:

- Expiration, history or reuse, and complexity.
- Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
- A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.
- Passwords must not be disclosed to other workforce members or individuals, including family members.
- Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
- Employees should refuse all offers by software, web browsers, and/or Internet sites to automatically login the next time that they access those resources.

5. Security Certifications and Training

a) All senior information security personnel are required to attain and maintain appropriate industry security certifications and remain current with industry best practices and technology, at least annually and as required to maintain industry security certifications. Industry security certification requirements are captured in job descriptions.

b) A CISSP certification is required for senior security staff. Other certifications may include, but are not limited to: CISA, CISM, Security+. Staff must maintain certifications and remain current on industry best practices by attending training courses, conferences, webinars and vendor presentations.

F. SECURITY INCIDENT PROCEDURE

Delta Dental shall have a documented Security Incident Response Procedure detailing how it, starting with the Information Security Team, will quickly react, contain, and manage Security Incidents.

Appropriate Legal and Information Security personnel shall receive training on the Incident Response Procedure, reporting procedures, incident response playbooks, and cyber crisis management plans within 90 days of commencing their role. Refresher training shall occur annually. Incident management plans shall be reviewed and updated annually.

All Security Incidents shall be promptly investigated, mitigated, and contained. If criminal action is suspected, and in accordance with the Cyber Crisis Management Plan, the Privacy and Security Officers shall evaluate contacting the appropriate law enforcement and investigative authorities, which may include, but is not limited to, the police or the FBI.

Reports and communications shall be made without unreasonable delay in accordance with the requirements of applicable law and no later than 60 days after the discovery of an incident, unless otherwise directed by law enforcement orally or in writing, and include the necessary elements.

It is the responsibility of each Delta Dental employee or contractor to report potential HIPAA Breaches and Security Incidents to the contacts below:

Report the incident using LogicGate, Delta Dental's Governance, Risk, and Compliance tool. The tool can be accessed one of the following ways:

- Using the link on the front page of Radar;
- https://bit.ly/3A25DGf
- https://rhsc.logicgate.com/steps/2HuesRKw?token=rFgBaPhyOLuVrUbxKzssZTEVHdfxZbzi

Incident reporters should follow the applicable link, fill out and submit the Initial Privacy Intake form to the Legal Department (see also the procedure – "Reporting Potential HIPAA Breaches" on the Delta Dental intranet site. This process is also trained upon annually. The CISO and Privacy Officer are available to offer advice and assistance to users of information systems for the handling and reporting of potential HIPAA Breaches and Security Incidents in a timely manner. If the incident involves employee noncompliance, the Privacy and Security Officers may work with a designated contact in Human Resources to discuss the application of appropriate sanctions.

Reports of potential HIPAA Breaches and Security Incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing processes and/or security controls are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the Privacy and Security Officers to provide guidance on any procedural changes that may be required, as a result of the investigation of a Breach or Security Incident. All employees and contractors shall receive training annually on how to report incidents, and instructions shall be made available on the company intranet for reference at any time.

G. CONTINGENCY PLAN

Delta Dental is committed to maintaining formal practices for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems containing ePHI. Delta Dental shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

The organization includes business requirements for the availability of information systems when specifying the security requirements; and, where availability cannot be guaranteed using existing architectures, redundant components or architectures are considered along with the risks associated with implementing such redundancies.

The Risk Management department, in accordance with the requirements of the company's Business Continuity Plan, shall perform an annual business impact analysis assessment by engaging key stakeholders and system owners to determine availability of information systems.

1. <u>Data Backup Plan</u>

a. The CISO shall ensure that a data backup plan is implemented to create and maintain retrievable exact copies of ePHI; that backup processes are in place; and that all applicable access controls are enforced. Data retention policies and practices shall be in place to keep sensitive data storage to a minimum.

b. Incremental system backups must be performed on a daily basis, Monday through Friday, with full weekly backups of critical databases. Backup copies must be stored offsite, at a separate location from the primary data center location. Copies should be rotated offsite daily, Monday through Friday at a minimum. Backups must be retained in compliance with data retention policies and with the backup plan procedure.

The CISO shall ensure backup procedures are tested annually to confirm that exact copies of ePHI can be retrieved and made available. To the extent such testing indicates need for improvement in backup procedures, the appropriate team(s) shall identify and implement such improvements in a timely manner.

2. <u>Disaster Recovery and Emergency Mode Operations Plan</u>

a. The CISO is responsible for ensuring that the written disaster recovery plan is annually updated for the purpose of:

i. Restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

b. The disaster recovery plan shall include the following:

   i. Current copies of the information systems inventory and network configuration developed and updated as part of Delta Dental's risk analysis.

   ii. Current copy of the written backup procedures developed and updated pursuant to this policy.

   iii. Identification of an emergency response team. Members of such team shall be responsible for the following:

      1. Determining the impact of a disaster and/or system unavailability on the entity's operations.

      2. In the event of a disaster, securing the site and providing ongoing physical security.

      3. Retrieving lost data.

      4. Identifying and implementing appropriate and effective "work-arounds" during such time information systems are unavailable.

      5. Taking such steps necessary to restore operations.

   iv. Procedures for responding to loss of electronic data including, but not limited to, retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of the risk analysis.

   v. Telephone numbers and/or Email addresses for all persons to be contacted in the event of a disaster, including the following:

      1. Members of the immediate response team,

      2. Facilities at which backup data is stored,

      3. Information systems vendors, and

      4. All current workforce members.

c. The disaster recovery team or equivalent shall meet at least annually to:

   i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Delta Dental;

   ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and

iii. Review the written disaster recovery plan and make appropriate changes to the plan. A team shall be designed and responsible for convening and maintaining minutes of such meetings. The designated team also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

H. SANCTIONS

Delta Dental shall apply appropriate sanctions against employees and contractors who fail to comply with security policies and procedures. Such sanctions may range from formal discussions with the individual's manager to immediate termination. A designated contact in Human Resources shall work with the Privacy and Security Officers as needed to handle the application of appropriate employee sanctions. The Human Resources department notifies staff management within 72 hours, when a formal sanction process has been initiated. Please refer to the TriState Privacy Policies, for further detail.

I. BUSINESS ASSOCIATE AGREEMENTS AND VENDOR MANAGEMENT

Delta Dental shall enter into Business Associate Agreements (BAAs) with any vendors, affiliates or other third parties, who may store, process, transmit, or access PHI. Delta Dental shall also ensure additional contractual security requirements are included with the standard agreements, commensurate with the services performed, whether connecting to the Delta Dental network or processing, storing or accessing ePHI including Strictly Confidential Information or Federal Government Confidential Information. Agreements shall specify access limitations; compliance auditing rights by representatives of Delta Dental's vendor management program or Information Security department; penalties; and the requirement to notify the organization whenever third-party personnel transfer or leave their roles (so Delta Dental system access can be timely terminated by Information Security).

Delta Dental shall also have a vendor management program in place to ensure vendors are in compliance with the Business Associate Agreements, additional contractual security requirements and any other service level agreements, as necessary. Vendors shall be evaluated upon initial procurement and re-evaluated periodically, in accordance with the assigned level of risk, based on the services provided. Such an evaluation shall consist of a security risk assessment, performed under the direction of the CISO, as well as regular internal progress meetings (occurring at an appropriate frequency, but no less frequent than annually) to review Vendor performance and identify and resolve any security or operational issues.

If applicable to the nature of the services provided, any access granted to Delta Dental's information and systems will not be permitted until due diligence has been performed, the appropriate controls have been implemented, and written agreements reflecting the security requirements and identifying and implementing appropriate controls and terms and conditions for access are signed acknowledging that vendors understand and accept their obligations and security risks, and indemnification obligations are clearly outlined. Agreements may also include language regarding geographic or other restrictions on the location of facilities that process, transmit or store covered information as needed, based on legal, regulatory, contractual and other security and privacy-related requirements. Delta Dental data privacy and security policies shall be provided and acknowledged by any non-employees (contractors, vendors) that access the in-scope environment. Where additional functionality is supplied which causes a security risk, the functionality shall be disabled or mitigated through application of additional controls.

Due diligence of prospective and current vendors may include, but is not limited to, interviews, document review, checklists, certification reviews (e.g., HITRUST) or other remote means. If a vendor is deemed critical in nature, due diligence may also include onsite visits.

Vendor contracts shall be reviewed before commencement of services or purchase of products and shall include acceptable language on information security measures to be implemented, the service levels to be achieved, and any other business considerations (including maintaining security during transitions and continuity following a failure or disaster).

Delta Dental shall develop, distribute, and periodically (at least annually) review and update a list of current vendors which shall include a description of the services provided.

To the extent that software development for in-scope systems is performed by a third party, contract language shall include a) licensing arrangements; b) code ownership and intellectual property rights; c) audit rights to determine quality and accuracy of work; d) escrow arrangements; e) quality and security functionality requirements for the developed code; and f) security testing and evaluation prior to installation. (For further detail, see the company's *Vendor Management Procedure*). Code reviews and other security reviews will be completed by the organization, in accordance with the Application Security Processes detailed in the Vulnerability Management Procedure.

For all system connections that allow customers to access Delta Dental's websites and portals, Delta Dental will provide appropriate text or a link to its privacy policy for data use and protection as well as the customer's responsibilities when accessing the data.

3. Physical Safeguards

Please refer to the Delta Dental Physical Security Policy for requirements regarding:

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

4. Technical Safeguards

The following sections are located in the Delta Dental Access Management Policy:

- User Accounts
- Password Complexity and Requirements
- Non-Interactive Accounts and Passwords
- National Provider File (NPF)
- Death Master File (DMF)

A. WORKSTATION, SYSTEM AND NETWORK REQUIREMENTS

1. **Host Workstation, Server and Application Configuration**

- All systems shall utilize industry standard anti-virus/anti-malware software with the following configuration:
    - Daily or "real-time" signature updates enabled which are updated automatically based on the approved update schedule settings.
    - Antivirus/anti-malware scans must be configured to scan upon boot and every 12 hours.
    - Antivirus/anti-malware Real time scanning should be configured where appropriate, scanning new file downloads/execution, ensuring any malicious files or code is blocked and quarantined with Information Security staff being alerted.
    - Anti-virus/Anti-Malware software shall be configured to monitor memory allocation with unauthorized code execution safeguards.
    - Every alert must be investigated by Information Security to confirm the validity and assess potential impact.
    - Must be centrally managed and tamper proof from non-administrators.
- All systems shall utilize industry standard personal firewalls.
- All systems shall use automated tools whenever possible to conduct configuration reviews.
- All systems with sensitive data shall be isolated (physically or logically) from non-sensitive applications/systems, unless the risk is identified and accepted by the owner.
- All systems shall be centrally managed, apply patches/updates from a central location, and be able to centrally verify configuration settings
- Web or Internet-facing systems shall utilize industry standard host-based intrusion detection systems (HIDS) or utilize file-integrity monitoring FIM), preferably both HIDS and FIM would be in place.
- All workstations must utilize Data Loss Prevention (DLP) software.
- All systems must utilize approved application whitelisting or blacklisting software.
    - Software outside of baseline images will need to be reviewed and approved by the Information Security team and reviewed annually.
- All systems' software and hardware shall be under a current and valid support contract with support service level agreements (SLAs) and response times, appropriate for the services performed by the systems.
- All systems shall be configured based on industry standard configurations, such as those available via the Center for Internet Security (CIS). Such standards shall include, but are not limited to:
    - Non-system administrator personnel shall be restricted from local administrative access on systems, preventing the installation of software.
    - Guest accounts must be disabled.
    - Default accounts and passwords must be changed.
    - Unused services and ports must be disabled.
    - USB and other removable media ports must be disabled via the use of technology controls.
        - Authorized users may write to Encrypted portable media
        - Authorized users require manager and CISO approval
        - Media copied to portable media must be labeled and restricted based off its classification.
        - DLP is required to record data transfers and maintains an inventory of media and the user that transferred the data. When no longer in use, disposal records must be logged and maintained.
        - Portable media may only be used to store sensitive data if encrypted.
    - All systems screensavers shall lock after a maximum **10 minutes**, forcing the user to re-authenticate to log back in.

- All systems shall have logon banners addressing the user's required authorized use, ownership, sensitivity of the systems and monitoring of user activity.
- Application session timeouts must be set to **30 minutes or less**. After timeout, the user must be forced to re-enter their password.
- All wireless-enabled devices (e.g., laptops / phones) shall have wireless file sharing (e.g., "Nearby Share" on Windows) disabled.
- Applications will retain separate authorization stores to prevent access rights from being shared between applications, unless otherwise required to do so.

2. <u>Network Architecture</u>

- All systems shall be protected by firewalls from public and other Untrusted Networks.
- Once a system has established a network connection (whether wireless or hard wired) authentication shall be required, prior to connecting to the local area network in which systems reside.
- MAC address authentication and static IP addresses for wireless and hard-wired connections shall be implemented.
- All systems must be segmented in an n-tier architecture with web-facing systems in the DMZ (a firewall in front of and a firewall behind the web-facing system), with functional systems in separate network segments, separated by logical or physical firewalls.
- The network perimeters shall be designed and implemented to require all outgoing network traffic to the Internet to pass through authenticated and filtered at the application layer. This traffic shall support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a blacklist. A whitelist of allowed sites that can be accessed while blocking all other sites shall also be supported.
- Internal directory services and internal IP addresses shall be protected and hidden from any external access.
- Router configurations shall be secured (e.g., access restrictions). The running (active) router configuration files shall be synced with the startup configuration files to ensure the intended secure settings are applied when the start-up configuration is run.
- Firewalls must limit traffic between network segments based on source IP address, destination IP address and the specific ports required.
- Firewall, router, and network connection changes shall be documented, tested, and approved prior to implementation.
- Exceptions to traffic flow shall be documented, and shall include business justification, risk assessment, and approval. These exceptions shall be reviewed annually (365 days).
- Firewall and router configuration standards, including wireless networks shall be formally documented. These standards include business justification for the use of all services, protocols, ports allowed, security requirements, and insecure protocols. These standards shall be reviewed at least every 6 months (180 days).
- Strictly Confidential Information and Federal Government Confidential Information may not be stored on systems in the DMZ without Encryption.
- Network-based Intrusion Detection or Prevention Systems (IDS/IPS) shall be used to monitor all networks in which systems are located which signatures are updated automatically based on the approved update schedule settings.
- Web Application Firewalls (WAF) shall be placed within the DMZ and used to monitor and protect systems from intrusions and attacks such as SQL injections which signatures are updated automatically based on the approved update schedule settings.
- A network diagram shall exist, which includes any wireless networks. The diagram shall be updated at least every 6 months and include any changes from the past 6 months.
- A connections / interface inventory or diagram shall exist that documents the following for each connection:
    i) the interface characteristics,

ii) security requirements,
iii) nature of the information communicated

- A network vulnerability scan shall be run at least quarterly to identify unauthorized components/devices.
- Delta Dental shall implement firewalls from at least two different vendors that employ stateful packet inspection technology. These firewalls can be network based or host based.
- Configurations shall have default-deny settings via host-based/network firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed
- Delta Dental shall implement at least two DNS servers that are placed on different subnets, which are geographically separated and perform different roles (internal and external) to eliminate single points of failure and enhance redundancy.
- A subnet shall be used to design / update network security policies (e.g., server remapping) when moving applications to virtualized servers.
- Network security processes shall be audited (e.g., internal or external assessments) or otherwise monitored to help verify the internal department or third party is following documented procedures
- Management shall ensure coordination of and consistency (e.g., review of network infrastructure configurations) in the elements of the network infrastructure
- DNS Servers with internal roles shall only process name and address resolution requests from within organizations. DNS Servers with external roles shall only process name and address resolution information requests from clients external to the organization (i.e., on external networks including the Internet)
- Network devices with dial-up capabilities shall not be procured wherever possible. If unavoidable, dial-up capabilities shall be disabled and review of the disabled status performed yearly to ensure compliance.

3. Separation of Environments

- Production environments must be separated from development, test and User Acceptance Testing (UAT) environments, where practical.
- Environments shall be logically separated at a minimum. The preferred method is physical separation.
- Software shall be migrated through the company's "Development", "UAT" then "Production" environments

4. Unified Communications

- Delta Dental shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously
- Delta Dental shall authorize, monitor, and control the use of VoIP within the information system
- Delta Dental shall ensure VoIP equipment used to transmit or discuss sensitive information is protected with FIPS-validated encryption standards

B. ENCRYPTION

Delta Dental shall implement technical security measures to guard against unauthorized access to sensitive data (e.g., PHI/PII, etc.) that is being transmitted over an Untrusted Network or is stored on electronic media. All Strictly Confidential Information, Federal Government Confidential Information and passwords shall be Encrypted as follows:

- Electronic transmissions must Encrypt data at a minimum of **128-bit** Encryption, with preferred Encryption of **256-bit**.
- Storage at rest on electronic media must be Encrypted at a minimum of **256-bit** Encryption.

Asymmetric key lengths shall be **2048-bit**.

All Encryption algorithms must be FIPS 140-2 compliant.

In the event electronic transmissions or storage at rest on electronic media cannot be encrypted, an exception must be submitted via the Variance Request Process to document, evaluate and accept the risk (or the transmission or electronic media may not be utilized).

C. KEY MANAGEMENT

Delta Dental shall have key management processes and procedures in place to manage Encryption keys. To ensure the protection, appropriate use and disclosure of keys, keys shall be:

- Inventoried and documented, along with their designated Key Custodians.
- Retired or replaced when:
    - The integrity of the key has been weakened, including when someone with knowledge of the key has left Delta Dental
    - The key is suspected or known to be compromised
- Changed periodically (where practical)
- Restricted in access to the minimum necessary personnel, based on their job function
- Stored securely in the lowest practical number of locations and forms

Key-Encrypting keys shall be:

- At least as strong as the data Encryption keys they protect
- Stored separately from data Encrypting keys
- Public and private cloud keys: Keys shall be managed by Delta Dental, based on cloud provider best practices
- Key rotation shall be in compliance with this policy
- Key ownership shall be defined
- Keys shall be backed up, highly available and part of the applicable disaster recovery plan

Key management practices must be NIST-compliant.

D. INTERNAL PROJECT RISK MANAGEMENT

Information security shall be integrated into Delta Dental's project management methods to ensure that information security risks are identified and addressed as part of all projects, including (but not limited to) projects for a core business process, IT, facility management, or other supporting processes.

Information security and privacy shall be addressed in all phases of project management methodology, including following:

(i) Information security objectives are included in project objectives

(ii) An information security risk assessment is conducted at an early stage of the project to identify necessary controls

E. APPLICATION SECURITY PROGRAM

If performing software development, Delta Dental shall implement and maintain an application security (AppSec) program to identify and document the functions, ports, protocols, and services intended for organizational use for detection, prevention, and remediation of application vulnerabilities and ensure data integrity for internally developed applications, and their 3rd party dependencies ("threat modeling"), early in and throughout the software development lifecycle (SDLC).

Delta Dental shall apply information system security engineering principles in the specification, design, development, implementation, and modification of security requirements and controls in developed and acquired information systems. Prior to production release, applications (including application programming interfaces - APIs) must conduct all of the required security assessments at least once.

a. Design Reviews - assessing design plans to flag security issues prior to the implementation of application code or infrastructure and requiring system developer(s) to provide control design and implementation information. Where possible, development and use of programs/routines that do not require elevated privileges is preferred. Least privilege principles shall be in place throughout application permissions, profiles and menus.
b. Detailed Test Plans - covering various types of testing (e.g., unit testing, static code analysis, data flow analysis, metrics analysis, peer code reviews)
c. Static Application Security Testing (SAST) - scans for code flaws and vulnerabilities.
d. Dynamic Application Security Testing (DAST) - scans applications at run time for vulnerabilities.
e. Penetration Testing - a manual test on a live application to simulate real-world threats such as privileged escalation attempts which may allow unauthorized access into other systems or applications.
f. Manual Validation Testing – testing for a specific vulnerability on a live application.
g. Outputs from application systems handling covered information are limited to the minimum necessary and sent only to authorized terminals/locations.

The applications subject to these assessments meet the following criteria: new releases, major upgrades, material or significant system changes, third party or acquired applications, point releases, patch releases, or emergency releases. Code that is not tested will not be a candidate to promote from lower environments. Code being promoted should follow the standard business pipeline process.

F. PATCH AND VULNERABILITY MANAGEMENT

1. **Patch Management**

- Delta Dental shall develop, document and comply with a patch management process covering all systems, whether on premises or in the cloud. Delta Dental's patch management program shall include alerts or notifications from industry standard services (e.g., US-CERT) and software providers (e.g., Microsoft, Oracle, Cisco, etc.).
- Security patches must be applied in a timeframe appropriate to the severity rating of the patch, where the severity is defined by US-CERT/National Institute of Standards (NIST) or software vendor. Specifically, security patches shall be applied within:
    - Two (2) weeks for critical severity rated security patches
    - One (1) month for high rated security patches
    - Two (2) months for medium rated security patches
    - Three (3) months for low rated security patches
- Security patches are not applied automatically. Security patches are tested before deploying to all systems, applications, and workstations, including all systems in the DR site within 2 weeks of being applied to the production environment.
- Security patches that cannot be applied due to software or hardware compatibility shall be documented as exceptions, with mitigating controls implemented to limit the exposure for the systems in which the security patch was not applied.

2. **System and Application Requirements and Vulnerability Management**

- Delta Dental shall develop, document and comply with a vulnerability management program, which is evaluated quarterly. Vulnerability assessments must be performed and reviewed by qualified Security resources.
- Web applications and systems, whether on-premises or in the cloud, developed or managed by Delta Dental and/or Delta Dental's subcontractors must be compliant with applicable security and privacy policies, standards and the secure coding checklist.
- Mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations) within browsers shall be restricted to the highest possible security settings, or blocked entirely if not necessary. Any outdated technologies such as postscript, shockwave movies, and flash animations shall not be allowed. PDF, Java, JavaScript shall be allowed but will be configured as securely as possible to mitigate any risks. ActiveX is currently allowed, but is in the process of being phased out. As soon as it is determined that ActiveX is no longer needed, it shall be blocked.
- When mobile code performs unauthorized actions, the executing mobile code shall be blocked or quarantined depending on the severity of the action.
- All systems shall be protected from unauthorized changes.
- All systems shall utilize the highest level of protocols (TLS 1.2 or greater).
- All information systems and network devices shall be hardened and configured based on industry standard configurations, such as those available via the Center for Internet Security (CIS).
    - CIS benchmarks include, but are not limited to, Level 1, Level 2, and STIG as tied to industry compliance standards
    - CIS benchmarks are reviewed annually
    - Any changes to the baseline should be entered as a documented variance with proper approvals added
- Systems will be scanned at a regular interval to ensure minimum baseline configurations remain in accordance with industry best practices and corporate minimum baselines
- Baseline configuration installation checklists (or equivalent) are used during the server and workstation build process to ensure minimum configuration standards are applied.
- Systems shall be set up so that product information on current and existing vulnerabilities (e.g., mailing lists, vendor notifications, website, etc.) are received, and systems are maintained when new or useful resources are found.

- Security personnel shall keep up to date with the latest security vulnerabilities, and trends as reasonably as possible permitting time and workload. As new knowledge is acquired and systems change, these new findings shall be assessed and incorporated as necessary into the company's standards and protection mechanisms.
- Software developers and contractors shall receive additional training and education in secure coding and the secure coding checklist.
- All systems shall undergo industry standard vulnerability scanning at least:
    - **Weekly** for external or Internet-facing systems
    - **Weekly** for internal or non-Internet-facing systems
    - **Immediately** when significant changes are made to a system.
- Prior to any vulnerability scans, the scanning tool must be up to date with the latest definition files. A list of all vulnerabilities must be maintained and kept for a minimum of 30 days and updated when new vulnerabilities are identified. High risk vulnerabilities must be verified through logs to determine if the vulnerability has been exploited.
- Vulnerability reports must include the scope of systems and/or components included for and vulnerabilities scanned for can be identified.
- Any unauthorized components or devices shall be scanned for and reviewed weekly. Any components or devices identified shall be shut down and access removed.
- Web applications developed by Delta Dental or Delta Dental subcontractors must undergo static application security testing (SAST) and dynamic application security testing (DAST), at least **twice each calendar year**. Any application systems, which are web or Internet-facing, custom or proprietary, accept field inputs and process Strictly Confidential Information or Federal Government Confidential Information, must be tested. Manual application penetration testing shall be performed on new web applications, and on existing web applications in which significant modifications have been made, prior to the release.
- SAST and DAST scans must include checks for common application vulnerabilities, including those within the Open Web Application Security Project (OWASP) Top Ten.
- In house, developed code must undergo data input validity checks and error checking is performed for fields allowing for data input. This should include format, data type, size and acceptable ranges.
- Software developers designing, coding and supporting web applications must receive **annual** secure coding training and adhere to documented secure coding checklists and standards.
- Delta Dental shall perform network penetration testing on systems **once per calendar year**. Testing shall be performed by a reputable third party.
- Vulnerabilities identified as a result of the scanning and testing performed in this section, shall be evaluated for risk, prioritized and resolved within:
    - Two (2) weeks for critical severity rated vulnerabilities
    - One (1) month for high rated vulnerabilities
    - Two (2) months for medium rated vulnerabilities
    - Three (3) months for low rated vulnerabilities

3. Certification and Accreditation

Prior to production release, all systems, software, containers, APIs and applications must be reviewed and scanned by the applicable Information Security Team, to ensure the minimum security requirements are present.

This includes design, patching, configuration standards validation, and vulnerability scanning. Any non-compliant items shall be remediated, prior to release or go-live. Exceptions may be required if specific configurations or patches impact the required business functionality of the system.

G. SOFTWARE OWNERSHIP

All software installed on Delta Dental systems must have an owner. If the software is not managed or supported by Delta Dental's IT organization, the owner is responsible for the following:

- Compliance with license agreement
- Only required staff have access and/or software installed
- Use of sensitive data is in compliance with this policy (e.g., local or cloud usage)
- Ensure Delta Dental's Procurement Department is appropriately engaged and aware of the software purchase and vendor's support.
- A formalized migration plan in the event the software becomes unsupported
- Ensure Delta Dental's Privacy and Security Officers are aware of any sensitive data usage
- Ensure software is patched, securely configured and otherwise maintained
- Review access and/or installation of software twice a year
- Ensure department executive has awareness of this policy and further, the department executive must own, evaluate and accept any associated business risk associated with any non-compliance or unmitigated security risks.
- Ensure that sensitive systems are isolated (physically or logically) from non-sensitive applications/systems unless the risk is identified and accepted.

For requirements regarding software that is managed or supported by Delta Dental, please see Delta Dental's Software Management Policy.

H. THIRD PARTY SERVICES OWNERSHIP

All third-party services (e.g., Software as a Service - SaaS), integrating with Delta Dental systems and/or storing, processing, or used in the transition of sensitive data, must have an owner. If the service is not managed or supported by Delta Dental's IT organization, the owner is responsible for the following:

- Compliance with any applicable services agreement
- Use of sensitive data, connectivity to Delta Dental systems and/or Delta Dental customer integrations is in compliance with this policy with prior authorization from the CISO
- Ensure the Procurement Department and Legal (Compliance Office, Privacy Officer) are all appropriately engaged and aware of this service
- Submitting the product or service to, and receiving approval from, the company's Architecture Review Council & Architecture Review Board (ARC/ARB) before purchase and implementation.
- Ensure any Delta Dental responsibilities (e.g., users, security configuration) are maintained
- If the third party is providing software development, all security flaws are tracked and reported to organizational defined personnel.
- Access to all systems or applications the third party interacts with is logged and monitored.
- Access provisioned for third party services is reviewed and approved by the third-party service's management, along with Delta Dental's Human Resources, Information Security, and Legal departments.
- Manage and maintain access as applicable
    - Review access at least twice a year
- Ensure department executive has awareness of this policy and further, the department executive must own, evaluate and accept any associated business risk associated with any non-compliance or unmitigated security risks.

For any new or material changes to enterprise architecture, Delta Dental shall ensure that information security is considered, including risk to Delta Dental's operations, assets, and staff, as well as other organizations (e.g., customers, partners, third parties). Further, as a result of enterprise architecture

changes, the information security architecture is reviewed and updated, with changes reflected in the security plan, procurement and acquisition processes.

I. WIRELESS ACCESS

- To the extent Delta Dental utilizes wireless (802.11) to access systems, wireless access points must adhere to the following minimum configuration standards:
    - All Wireless Access Points (WAPs) must be inventoried, business justified and approved for use.
    - All Wireless Access Points must be centrally managed and have default passwords, SNMP strings and encryption keys changed prior to production use. All passwords, SNMP strings and encryption keys must be changed when a Wireless administrator leaves that position or company.
    - Wireless Access Points must be placed in secured locations to avoid tampering.
    - Shutting down Wireless Access Points when not in use is not applicable due to employees working at night and weekends.
    - Rogue access point detection is required and scanned for at least quarterly. If a rogue access point is detected it shall be blocked by MAC address.
    - Utilize Encryption (WPA2 or highest standard supported)
    - Encryption should be AES-256 bit or higher
    - Ensure only authorized devices may connect to the network, using device authentication where possible. Wireless access must be monitored for unauthorized devices.
    - Wireless network must be segmented via firewall
    - Once wireless connection is established, authentication shall be required, prior to connecting to the local area network in which systems reside
    - Guest wireless access must be segmented from Delta Dental networks, only permitting Internet access
    - Connectivity must be protected by Delta Dental firewall(s), IDS/IPS and URL filtering
    - Audit logging must be forwarded to the appropriate Delta Dental log management/security information and event management (SIEM) solution

J. REMOTE ACCESS

- Delta Dental shall limit the ability for remote access into the network which supports Delta Dental systems. Such access shall be limited to authorized personnel only.
- Delta Dental shall utilize Encryption to secure and protect remote access connections.
- End users authenticating over a public network shall connect remotely to the Delta Dental VPN
- End users shall ensure critical files are backed up to company-approved locations (e.g., personal file shares on company network, OneDrive) and comply with business continuity directives.
- Delta Dental will prohibit data transfer functionality (copy, print, save) when remotely accessing sensitive data, without a defined business need. If it is deemed necessary, the justification shall be documented with approval rationale.
- Delta Dental shall require two-factor authentication to utilize remote access.
- Delta Dental shall not permit split-tunneling or simultaneous access to the Delta Dental network and any other network. One standard exception is Microsoft Teams.

- Delta Dental shall actively monitor for attempts from unauthorized devices to gain remote access. All access to third parties' services/systems, cloud applications, and any other systems not hosted by Delta Dental and processing storing, transmitting or access sensitive data; must:
    - Route connectivity through the Delta Dental network via firewall or cloud access security broker (CASB). This ensures all data and system activity is appropriate monitored and protected.
    - Where possible, restrict access to resource from only company-managed devices

K. AUDIT LOGGING AND MONITORING

Delta Dental must implement application, hardware, software, and/or procedural mechanisms which record and examine activity in information systems that contain Strictly Confidential Information or Federal Government Confidential Information. Audit controls are technical mechanisms which track and record computer activity. An audit trail determines if a security violation occurred by providing a chronological series of logged system events that relate to an operating system, an application, or user actions.

Delta Dental routinely audits users' activities in order to continually assess potential risks and vulnerabilities to Confidential Information in its possession.

- Delta Dental shall develop audit logging and log monitoring procedures, which include the capturing and aggregating of audit logs in a central audit logging solution / SIEM. Security audit activities shall always remain independent.
- Delta Dental audit logs shall consist of all relevant security event logs for the systems, as determined by the CISO, security risk assessments, and cybersecurity risk mitigation strategy. This includes logs from systems and devices including, but not limited to: firewalls, IDS/IPS, authentication systems, applications, databases and VPN devices.
- Delta Dental shall log actions for privileged accounts. These logs shall contain the following information:
    - Information about the event (e.g., files accessed, functions performed),
    - Success/failure of the event,
    - Time the event occurred, information about the event (e.g., files handled) or failure,
    - The account or administrator involved, and
    - Which processes were involved.
- Audit log monitoring shall include correlation of events and the generation of alerts and escalation to applicable information security resources in a timely manner, including monitoring of security events by Delta Dental security personnel during business hours, as well as on-call support to respond to escalated security alerts, from a third party security firm, twenty-four (24) hours a day, seven (7) days a week, three-hundred and sixty-five (365) days a year, in the event of critical or high severity security alerts.
- Audit log monitoring KPI's will be reviewed annually by security personnel whose primary responsibility is to administer and maintain the logging system/SIEM.
- Security Administrators shall not administer logging software, nor perform the log reviews of administrator activities to achieve separation of duties. Systems shall maintain synchronized time to ensure adequate support for accurate correlation of events across systems, applications, and network devices.
- Separation of duties.
- No single person shall be able to access, modify or use systems without authorization or detection.
- Audit log entries should utilize write-once or tamper-proof capabilities to ensure logs cannot be modified.

- Audit log events shall include sufficient level required to support forensics investigations. Such detail may include, but is not limited to:
    - Timestamp,
    - Source IP address,
    - Destination IP address,
    - System name,
    - Username and unique user ID,
    - System or application process ID,
    - Description of error and activity or function performed
    - Filename accessed
    - Program or command used to initiate the event
- The types of audit log activities shall include, but not be limited to:
    - Dates, times, and details of key events (e.g., log-on and log-off);
    - Records of successful and rejected system access attempts;
    - Records of successful and rejected data and other resource access attempts;
    - Changes to system configuration and procedures for managing configuration changes;
    - Use of privileges;
    - Use of system utilities and applications;
    - Files accessed and the kind of access;
    - Network addresses and protocols;
    - Alarms raised by the access control system;
    - Activation and de-activation of protection systems, including anti-virus systems and intrusion detection systems, and identification and authentication mechanisms,
    - Creation and deletion of system level objects, and
    - File Integrity monitoring
- At a minimum, the following user activities shall be logged for all in-scope applications and databases:
    - Create
    - Read / View
    - Update / Edit / Modify
    - Delete
- Sensitive data shall be logged with date, time, and recipient/sender.
- Audit logs shall be retained for at least **one (1) year**, or as specified in the applicable records retention policy or other applicable law, whichever retention period is longer. If involved in an investigation, logs must be retained until investigation is completed.
- Correlated events generated using selectable criteria from audit, security, or application alerts are to be tracked for trending analysis and evaluation. If an appropriate risk is identified, the findings are tracked, documented, and investigated.
- Extracts of sensitive data exports (such as uploads to FTP sites) shall be verified every 90 days to confirm if it's still required or can be deleted.
- Firewall rules shall be reviewed at least **once a year**.
- Firewalls and routers used to secure and manage the PCI cardholder data environments, require line-item reviews **twice a year**.

L. CHANGE MANAGEMENT

Delta Dental shall track all changes to networks, systems, and workstations, including software releases, which access, process, or store ePHI. The change management process shall occur in coordination with Delta Dental's risk management process. If a risk assessment has been conducted as a result of a significant change in the environment, or a change that could have a significant organizational impact, the results of such risk assessment shall be integrated into the change management process. All changes shall follow a documented approval process prior to implementation.

The following must be identified:

- asset(s) impacted,
- a summary of the changes,
- the user making the change,
- the approvers,
- the steps to implement the change, and
- back out procedures.

All changes that impact or may impact security controls (e.g., firewall rule changes), require Information Security's approval, prior to implementation.

All change control documentation must be retained for at least **two (2) years** within a ticketing system. After two years, change documentation will be archived.

All source code assets are stored within a version control system and made available for use in rollback scenarios if required.

All changes capable of testing prior to production deployments must be tested prior to implementation.

M. DATA INTEGRITY

Delta Dental shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been modified or destroyed in an unauthorized manner. Possible electronic mechanisms for authentication may include (but are not limited to) error-correcting memory, magnetic disk storage, digital signatures, encryption, batch processing, and check sum technologies.

Where practical, Delta Dental shall utilize applications or manual procedures to validate that data received from a data supplier, customer or partner, is complete and unaltered.

Delta Dental shall integrate and embed throughout the entire end-to-end certificate/signature management process through approved trusted sources.

APPENDIX A – DEFINITIONS

TERM	DEFINITION
Data Owner	Each department that maintains or is responsible for patient health records, either in electronic or paper form, is required to designate a

	records management coordinator who will ensure that records in their area are preserved, maintained, and retained in compliance with established records management policies and retention schedules. This individual will also ensure the appropriate and authorized access to their data sets.
Electronic Protected Health Information (ePHI)	PHI that is in electronic format.
Encryption	The process of transforming information, using an industry standard algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.' To read an encrypted file, requires access to a secret key or password which enables it to be decrypted. Unencrypted data is called plain text; encrypted data is referred to as cipher text.
Information Systems or Systems	Any Delta Dental-owned or maintained networks, servers, containers, APIs, applications, workstations or devices hosting or used to access, process or view Confidential Information, Strictly Confidential Information, or Federal Government Confidential Information; or systems providing services to or on behalf of Delta Dental. Systems include systems utilized by subcontractors to provide services to Delta Dental.
Key Custodian	The individual assigned the responsibility to maintain Encryption keys. This includes ensuring the keys are limited to only authorized users, the keys are updated per policy, as well as ensuring the keys are available, in the event of a disaster.
Masked	Data in which the PHI, PII, or password fields are replaced, with other randomly generated values or scrambled, to disguise the values. Masked data is not necessarily de-identified data under HIPAA, as defined in 45 CFR 164.514(a) & (b).
Personally Identifiable Information (PII)	Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.
Protected Health Information (PHI)	Individually identifiable health information that is in any form or media, whether electronic, paper, or oral. PHI shall have the same meaning as the term "protected health information" as defined in 45 CFR 160.103, limited to the information created, received or accessed by a Business Associate from or on behalf of a Covered Entity.
Security Incident	Under the HIPAA Security Rule, a Security Incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Untrusted Network	A network that is not managed by Delta Dental personnel and/or in a Delta Dental facility. Typically used to refer to the Internet.

APPENDIX B – DATA CLASSIFICATION

	Strictly Confidential Information	Federal Government Confidential Information	Company Confidential Information	Public Information
Definition	Information related to individuals and critical business operations. Inappropriate release, loss or corruption would have a significant negative impact on Delta Dental, its affiliates, customers, members, suppliers, partners or employees.	Information related to individuals associated with the Federal Government Programs. Inappropriate release, loss or corruption would have a significant negative impact on Delta Dental, its affiliates, customers, members, suppliers, partners or employees.	Information that may be proprietary, indicate how Delta Dental business is conducted and client information. If the Information is lost, inappropriately released or corrupted; the result may have a negative impact on company business operations, financial risk and legal liability.	Information that is not confidential and can be made generally available to the public without any implications to Delta Dental.
Confidentiality	High	High	Moderate	Low
Availability	High	High	Moderate	Low
Integrity	High	High	Moderate	Low
Access Requirements	Delta Dental affiliates, customers, partners, members with minimum necessary and need-to-know based on job function. Where appropriate, Business Associate agreements and non-disclosure agreements	Delta Dental personnel or contactors with minimum necessary and need-to-know based on job function. Access requires ADP I or ADP II clearance.	Delta Dental affiliates, customers, partners and vendors with a need-to-know and signed non-disclosure agreements	Delta Dental affiliates, customers, partners and the general public

Examples	• Individual identifiable Information such as:
	  ○ Social Security Numbers
	  ○ Credit card Number
	  ○ Healthcare/Dental Identification numbers
	  ○ Date of birth
	• Account names and passwords
	• Information that has the potential to provide a competitive advantage
	• Information about potential company acquisitions
		• Individual identifiable Information related to Federal Government Programs such as:
		  ○ Social Security numbers
		  ○ Credit card number
		  ○ Healthcare/Dental Identification Numbers
		  ○ Date of birth
		• Account names and passwords
			• Information about clients, including their status, initiatives, organizational changes
			• Internally communicated information including operating procedures, policies and notices.
			• Trade secrets
			• Organizational charts and personnel contact information.
			• Employee lists
			• Pricing information
			• Contracts
			• Internal diagrams such as network and data flow
			• Security program information
				• Information available on our public facing websites, such as annual report publications, press releases
				• Interviews with news media
				• Business cards
				• Company brochures widely distributed for prospective members

APPENDIX C – CLASSIFICATION LABELS

Within Microsoft Office applications (Word, Excel, PowerPoint, Outlook) you will see various labels to classify your documents and content:

- **Non-Business:** Information that does not belong to the organization or is personal (ex. Email to daycare, Grocery list)
- **Public (as defined in Appendix B)**: Information that is approved to be viewed by anyone in the world (ex. Advertisement)
- **Internal**: Information that should not be shared externally and is not confidential (ex. Email to co-worker, Presentation)
- **External**: Information that will be shared externally but is not confidential. (ex. Meeting with customer, generic document)
- **Confidential (as defined in Appendix B)**: Information that is sensitive, but does not contain PII/PHI; Will apply a header, and footer and external offline access will expire after 7 days (ex. Documentation, Email about inner workings of the organization)
- **Federal (as defined in Appendix B)**: Information that has federal government data within it; Will apply a header, and footer and offline access will expire after 7 days (ex. Audit information)
- **Strict (as defined in Appendix B)**: Information that contains PII/PHI or other extremely sensitive data. Will apply a header, and footer and offline access will expire after 7 days (ex. Patient record, Blueprint)
- **Custom**: Lets you define the protection and expiration for the item as you see fit. (ex. Give a person “view” only access for 1 week)