Delta Dental Plan of Michigan, Ohio, and Indiana

Access Management Policy

Procedure #: 435-07	**Title:** Access Management 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			

Contents

Revision History

NAME	DATE	VERSION	SUMMARY OF CHANGES
Andrew Woodard, Meredith Sharp	07/11/2017	1.0	Initial Draft
William Schrader	3/19/2018	1.1	Interactive Account Update
Andrew Woodard, Meredith Sharp, RHSC Security Council	October 17, 2018	2.0	Revisions for RHSC Enterprise-wide Policy Updates
Andrew Woodard, Meredith Sharp, RHSC Security Council	January 15, 2020	2.1	Annual Review and Updates
Meredith Sharp, Andrew Woodard	May 14, 2020	2.2	Addition of language regarding recording of meetings; Removal of clearinghouse language
Meredith Sharp	October 19, 2020	2.3	Addition of Death Master File language
Meredith Sharp, Andrew Woodard	February 11, 2022	3.0	HITRUST updates
Meredith Sharp, Andrew Woodard	March 28, 2023	3.1	Annual Review and HITRUST Updates

Approval History

NAME	DATE	VERSION	SUMMARY OF CHANGES
Data Privacy Committee	07/11/2017	1.0	Initial Draft
RHSC Executive Cybersecurity Committee	October 17, 2018	2.0	Revisions for RHSC Enterprise-wide Policy Updates
RHSC Executive Cybersecurity Committee	January 15, 2020	2.1	Annual Review and Updates
RHSC Executive Cybersecurity Committee	March 23, 2021	2.3	Addition of Death Master File language
Compliance Committee and Data Governance & Protection Council	February 11, 2022	3.0	Revisions for HITRUST compliance
Compliance Committee and Data Governance & Protection Council	March 28, 2023	3.1	Annual Review

Purpose

This policy specifies the formal processes and procedures in place to authorize access to Confidential Information and Systems (as defined in the Information Security Policies). This document addresses additional content intentionally not addressed in the Delta Dental Information Security Policy.

Scope

- All Delta Dental employees, contractors, vendors and consultants (individually or collectively referred to as "Personnel"). Where applicable, the requirements of this policy shall also apply to customers.
- All locations where Personnel are working on behalf of Delta Dental or any Delta Dental client.
- All computer and data communication systems, networks, applications, and data owned by or administered by Delta Dental or any of its affiliated entities, or designated vendors.
- Personnel conducting company business using authorized personal equipment.

Policy

WORKFORCE SECURITY

Delta Dental shall restrict access to Confidential Information to the appropriate staff members. The access control system for the system components storing, processing or transmitting covered information is set with a default "deny-all" setting. Delta Dental shall prohibit any other Personnel from unauthorized access to Confidential Information.

Accordingly, the following processes and activities shall be in place:

1. **Minimum Necessary Access**

   Delta Dental ensures all access to Confidential Information is based on need-to-know and is restricted to users based on the minimum necessary amount of Confidential Information, Strictly Confidential Information and Federal Government Confidential Information; required to perform their job function. Further, all job functions must have corresponding descriptions detailing the work the staff member must perform, which may require access to Confidential Information.

2. **Separation of Duties**

   There shall be separation of duties for critical functions, tasks or approvals performed for individuals in sensitive areas, to ensure no single individual has end-to-end control of a process, without an independent checkpoint.

3. **Software Development Access to Production Systems and Data**

   Access to production systems and Strictly Confidential Information or Federal Government Confidential Information shall be limited based on the user's job function. As is best practice, software development staff should not have access to production systems and corresponding

data, including the system or application permissions enabling Personnel to make changes to the environment or make changes to production software or code.

Where practical, software development staff shall only have access to Masked Strictly Confidential Information or Federal Government Confidential Information.

In the event software development staff access is required for ongoing support or application outages or issue investigations, such access shall be limited to those individuals and approved by the user's manager. Access granted temporarily to investigate application production outages, shall be removed when no longer required.

4. Staff New Hires, Transfers and Terminations

NEW HIRES

All new hire access requests must be submitted via a Technical Assistance Center (TAC) ticket and email to Human Resources. Human Resources typically initiates this process by entering the new staff member into the master Human Resources personnel system. As part of the access request, managers must update the ticket to advise Information Security (and local account management staff) and the Helpdesk of the specific access that is required.

TRANSFERS

In the event a staff member takes another position within Delta Dental, the user's new and former managers must develop a transition plan, including timelines in which the user's systems access can be removed, when no longer performing their former position's tasks and responsibilities. The user's former manager must submit a TAC ticket to remove the access, including any physical access, which is no longer required. The user's new manager must also submit a separate ticket, if one is not submitted by Human Resources, to ensure the user's new access is set up appropriately. There may be position transfers (e.g. intra-department), which may not require a change in access.

TERMINATION

Upon termination of an employee or contractor, whether voluntary or involuntary, the employee's manager shall work with Human Resources to enable prompt notification to Facilities and the appropriate Information Security team to remove the user's logical access to Delta Dental systems and physical access to Delta Dental offices. Notification to these teams shall require a TAC ticket, and may require an Email or phone call to the appropriate staff, in the event of an immediate termination. Depending on the organization, the employee's or contractor's manager or Human Resources is responsible for ensuring that all Delta Dental assets are returned, including but not limited to: keys, photo ID/key card badges, laptops, smartphones and any other company-issued items, prior to the manager escorting the staff member out of the office on their last day of employment at Delta Dental (if the employee is working on-site). In addition, personal devices (e.g. smartphone, tablet) must disconnect from any corporate assets, such as company Email. Please refer to the Mobile Device Policy. For any Personnel who are remote at the time of their termination, all company-issued devices will be sent remote-wipe commands. For any Personnel with personal devices connecting to Company Systems, applicable profile deletion should be initiated to remove Company information off the device and remove connectivity.

INFORMATION ACCESS MANAGEMENT

Delta Dental is committed to establishing and maintaining access to data, applications, systems, networks and network services in a manner that ensures maximized confidentiality, integrity, availability, protection, authenticity and utility for these resources. A mix of administrative, physical and technical controls must be in place. Delta Dental

requires formal processes and procedures be established to authorize access to Confidential Information and systems.

TECHNICAL ACCESS CONTROLS

User Accounts

Individual users (including customers and vendors) shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.
- Accounts may not be shared.

All user access is reviewed at least **quarterly**, and all accounts no longer required, are disabled. For the access review, the user's manager or the vendor relationship manager must approve their staff's access. If no response is provided to approve the access, the access will be disabled. Note, Director level staff and above can approve their own access. Delta Dental's Human Resources Department notifies designated ISS/IT and information security resources upon the departure of all employees and contractors, at which time logon IDs are disabled. Access reviews must be stored for at least one (1) year.

In the event customer-facing application user accounts (e.g. subscribers), or other internal-facing application user accounts, cannot be practically reviewed once or twice a year, accounts must be monitored for inactivity. After a specific interval of inactivity, accounts must be disabled.

- Customer user accounts must be disabled after **twelve (12) months** of inactivity for providers and benefit managers. Subscriber user accounts must be disabled after **eighteen (18) months** of inactivity.
- Employee and contractor Microsoft Active Directory accounts must be disabled after **ninety (90) days** of inactivity.
- Employee and contractor applications (e.g. NetIQ eDirectory) and database accounts must be disabled after **ninety (90) days** of inactivity.

All users must authenticate prior to being granted system access. The logon ID or account must lock after a maximum of **five (5)** unsuccessful login attempts, which then requires the account to be unlocked by the appropriate system administrator. As an alternative, the account should at least remain locked for a minimum of 30 minutes.

New account requests for new employees or contractors must be initiated by Delta Dental's Human Resources. All other access requests for systems and applications (including remote access), require a TAC ticket to be submitted by the user's manager. If the user's manager is not available, the next higher level of manager must submit the request. Please note that Director-level staff members and above may submit their own access requests. Model user is provided by manager to ensure correct roles are reviewed and granted by Information Security Admins with appropriate approvals. The manager or manager's delegate will deliver the credentials directly or contact the user's phone number on file to provide initial login credentials.

Where applicable, any third party user accounts used to access, support or maintain systems components remotely shall only be active for the duration required to conduct business. While the vendor account is active, it shall be monitored, and disabled upon complete of the support task.

All access requests must be entered into a tracking system.

Security Administrators (or staff performing identity management requests) shall review all access requests as they are processed and review access at least semi-annually to ensure the access requested is appropriate based on the user's job function. If the access appears to be above and beyond what should be appropriate for this job function, the Security Administrator shall request the user's manager to provide a business justification for the level of access requested. If the Security Administrator determines the business justification is not sufficient for the level of access required, they will escalate to the CISO for approval. A list of employees, contractors, and vendors with access to customer PII is maintained through the access groups derived during the review.

Password Complexity and Requirements

User IDs and passwords are required in order to gain access to all Delta Dental networks and systems. All passwords must be strong passwords. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. When passwords are initially set for new users or reset for existing users, the user will be automatically prompted to manually change that assigned password. Prior to resetting a user's password, the authorized individual with permissions to reset the password, must verify the user's identity, either in person via government issued identification or via phone, by validating previously obtained user-specific information (name, email address, phone number, manager, location/address, etc.).

The password requirements are:

- Password Length – Minimum of ten (10) characters
- Password Expiration – Every Ninety (90) days
- Complexity Content – Must contain at least one of each of the following:
    - Upper case letter
    - Lower case letter
    - Number
    - Special character (e.g. !, $, #)
- System Passwords Remembered - 24

Temporary passwords shall be generated in such a way that they are unique and non-guessable. Acknowledgement shall be obtained from a user upon receipt of a temporary password.

A password dictionary shall be in place. When users create / change passwords, the new passwords shall be checked against the dictionary. The dictionary shall be reviewed every 180 days.

Password expirations for customer users (e.g. subscribers, providers, partners), shall also expire periodically, where practical.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential. Passwords may be stored in password managers or vaults for individuals or team support requirements (such as disaster recovery). Such password vaults must encrypt the passwords and require an ID and password to access the password vault. Where possible, password manager access shall require multi-factor authentication.

Restrictions on Recording Passwords - Passwords must be Masked or suppressed on all login prompts or screens, and are never printed or included in reports or logs. Passwords must be stored in an Encrypted format.

Privileged Accounts

A privileged user account has elevated access, above that of a standard user account. Privileged users may have the ability to make administrative changes to operating systems, applications and databases. Examples of privileged user roles include: system administrators, database administrators, users with administrative access on a workstation, server or database. System Administrator (SA) accounts are used when someone needs elevated permissions that are not allowed on their standard network account. SA account creation requires manager approval with a ticket submitted to Information Security.

In addition, any users with direct access to databases are privileged users. This includes users who access the database with an Oracle client, SQL Developer or other similar clients, which bypass front-end web or client server applications.

Two-factor authentication is required for all remote access and privileged users. To enforce this policy, the two-factor authentication software client is installed on the privileged user's workstation. Where practical, the two-factor authentication client software must be installed on any workstation the privileged user may potentially use on the Delta Dental network.

For two-factor authentication users are set up with either a hard token, soft token, or a combination of both. If a hard token is requested by the end user, Information Security will set up a key fob and personally deliver the hard token to the user. If the user is not on-site the hard token will be mailed to the user-by-user services. If a soft token is requested, Information Security will send the end user instructions for them to set up the application on their phone and register their account.

Privileged access will not be assigned to any birthright access groups and must be explicitly requested.

Privileged user accounts must be reviewed every 60 days.

Non-Interactive Accounts and Passwords

Application service accounts, also known as non-interactive accounts, may not be used by an individual to interactively or manually log into applications, systems or databases. Any user accessing a Delta Dental system or application with a non-interactive account is subject to the sanctions policy. Individual user accounts may not be used for automated processes or running applications. Non-interactive accounts must be used in these cases.

All non-interactive account passwords must be changed **annually**. Additionally, temporary passwords for system accounts shall be required to be changed upon the first login, including temporary passwords provided during password resets. Passwords shall also be required to be changed immediately after an account compromise is detected.

Passwords cannot be stored in clear text and must be encrypted. Passwords shall not be stored in files, on web-facing systems, unless required by the native software or hardware. Passwords shall never be stored in automated log-on processes. (Note: this does not include SSO functionality). Password vaulting shall be used for all new applications developed by Delta Dental.

PKI-Based Authentication

When PKI-based authentication is used, the information system validates certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; enforces access to

the corresponding private key; maps the identity to the corresponding account of the individual or group; and implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

National Provider File

Due to the sensitive nature of the data contained within the National Provider File (NPF), access to the data shall be restricted to a need-to-know basis, based on the user's job function. A **quarterly** review shall be performed. This request will then be approved by the designated entity owner. The owner shall be an ISS/IT Manager or above.

Additionally, **annual** reviews shall be performed for access to the Delta Dental Plan Association's (DDPA) Administrator Portal and NPF Portal.

Death Master File

The Limited Death Master File (DMF) is an official government dataset of deceased citizens maintained by the Social Security Administration. It includes over 85 million death records, from 1936 to the present day. Due to the sensitive nature of the data contained within the DMF, access to the data shall be restricted to a need-to-know basis, based on the user's job function. Access will only be granted to those who have been determined to require the data to perform their job duties. Approved users will be required to undergo additional specialized training before being granted access to the DMF, in addition to annual training. Reviews of access and compliance shall be conducted at least annually for standard users, and semi-annually for privileged users.

Recording Conference Calls (Audio/Video)

Meetings can involve the discussion of confidential and sensitive topics. To limit access to Strictly Confidential Information or Federal Government Confidential Information. or other sensitive or confidential information, conference calls conducted using video-conferencing applications (including, but not limited to, Microsoft Teams, Zoom, or BlueJeans), whether involving internal Delta Dental staff or between Delta Dental staff and third parties, should not be recorded unless there is a legitimate business need.

If there is a business need to retain a recording of a conference call (e.g. a vendor demonstration of a third party product, or a staff training session):

- Approval must be granted by both the CISO and the Legal Department before recording any calls which will contain Strictly Confidential Information, Federal Government Confidential Information, or other regulated sensitive or confidential information.
- Appropriate agreements must be in place with the video conferencing application company before any calls are recorded.
- Recordings must be stored in an approved location with appropriate access controls.

  Please note: Microsoft Teams is the only approved conference call solution for recording.

Deviations

All requests for deviations from or exceptions to any Security policy must be approved by the CISO.

References and Related Policies

- Delta Dental Information Security Policy
- Code of Ethics and Conduct
- Acceptable Use Policy
- Mobile Device Policy
- Delta Dental Access review Procedure
- Delta Dental Employee Account Life-Cycle Standards