Policy: Confidentiality	Information Security & Privacy 01.105

New Hampshire Department of Health and Human Services
Bureau of Human Resource Management

Effective Date: 03/28/2005
Last Revision: 06/11/2020

Approved:

Lori A Weaver, Deputy Commissioner
Date: June 11, 2020

Last Reviewed by Information Services: 06/11/2020

Regulatory References:	References:
Regulation(s): Statute(s): RSA 91-A Admin Rules(s): PART Per 1002 DISCIPLINE	NIST SP 800-53 DHHS Data Classification Table

Section 1 - PURPOSE OF POLICY

1.1. The purpose of this policy is to provide Department staff with an understanding of their responsibilities to recognize and safeguard the data to which they have access and use as part of their employment or agreement with the Department. In the absence of any division/facility/bureau/program (business area) policy, this policy shall apply. In the event that a business area policy has fewer requirements or a less stringent policy or practice than is stated in this policy, this policy shall take precedence.

Section 2 – DEFINITIONS

2.1. Background Check – For the purposes of this policy, "Background Check" shall mean all types of criminal and civil background checks as required by the security policies of the federal agencies whose data the Department staff is authorized to access or handle.

2.2. Client - Any applicant for or recipient of benefits, programs, or services provided or administered by the Department.

2.3. Confidential Data – For the purposes of this policy, "Confidential Data" means all non-public information owned, managed, created, received from, or on behalf of, the Department that is protected by information security, privacy or confidentiality rules, and state and federal laws. This information includes, but is not limited to, derivative data, Protected Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information, Social Security Administration, and CJIS (Criminal Justice Information Services) data. Confidential data is classified as DC-3 or DC-2 data.

2.4. Contractor – Any individual or entity performing services for the Department under a written agreement, including the employees and sub-contractors of the individual or entity.

2.5 Criminal Records Check – A review conducted by the Department on each applicant selected for employment to include a review of: the Division of State Police NH Criminal History Record Information per RSA 106-B:14; the Bureau of Elderly & Adult Services State Registry per RSA 161-F:49; and the Division for Children, Youth & Families Central Registry per RSA 169-C:35.

2.6. Data Classification – Process to consistently organize and manage data based on its level of sensitivity, value, and criticality should that data be accessed, disclosed, altered, or destroyed without authorization. Data classification determines the levels of protection and controls required to safeguard the confidentiality (undisclosed), integrity (unaltered), and availability (accessible) of that data, reducing the risk of data events or breaches with financial, legal, and reputational implications.

2.7. Data Governance – A matrixed program that consists of all Data Stewards, Information Service Leads, and the Data Management Group. It was created to assure the consistency, confidentiality, integrity, and availability of New Hampshire data while promoting data sharing and interoperability.

2.8. Data Steward – Department employees identified by the Division Directors as having responsibility for the data management of the business processes such as access, storage, retention, distribution, or exchange of data.

2.9. Department – Department of Health & Human Services.

2.10. Department Employee – An individual working in an authorized Department position number.

2.11. Department Staff – Department employees, contractors, unpaid interns, and volunteers.

2.12. DoIT – The New Hampshire Department of Information Technology.

2.13 Facility – Any building or section of a building, leased by, assigned to, or owned by the Department, where Department business is conducted.

2.14. NIST – National Institute of Standards and Technology (NIST) is a non-regulatory government agency that provides standards and guidance for federal data security. In general, in return for receiving access to federal data the Department agrees to a variety of requirements including compliance with NIST standards and guidance.

2.15. Non-public: Regulated Confidential Data – Data regulated by State or Federal law and/or agreement. It shall also have the same meaning as "Confidential Data" as defined in this policy and is classified as "level 3" data (DC-3). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.16. Non-public: Restricted Data - Data <u>not</u> subject to release under Right to Know request per NH RSA Chapter 91:A. Such data may be released to an individual or entity subject to

proper authorization or proper redaction or suppression and is classified as "level 2" data (DC-2). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.17. Public: Non-published Data - Data subject to release under Right to Know request per RSA Chapter 91:A is classified as "level 1" data (DC-1). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.18. Public: Published Data - Data for which there is no expectation for privacy or confidentiality and therefore has been made available to the general public. It is classified as "level 0" data (DC-0). For further information on data classification, refer to the Department's Data Classification Policy and Table.

2.19. Right-to-Know – A New Hampshire statute that affects every aspect of government in the state of New Hampshire. The intent of the Right-to-Know (RTK) law (RSA 91-A-1) is to guarantee that the public has access to public records of all governmental bodies in the state of New Hampshire. To read the RTK law or to review exemptions to this law go to http://www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-5.htm.

2.20. Supervisor – The Department staff's immediate supervisor/Point-of-Contact or a person at a higher supervisory level within the Department staff's chain of management within the Department.

2.21. Unpaid Interns – A student who is enrolled in a post-secondary educational institution for the educational benefit of the student and has signed an unpaid internship agreement with the Department.

2.22. Volunteers –An individual who freely offers to undertake a service for the Department without compensation of any kind.

Section 3 - SCOPE

3.1. This policy applies to all Department staff.

Section 4 - POLICY STATEMENT

4.1. Safeguarding non-public regulated confidential data (DC-3) is a compliance requirement critical to the Department's operations. All information or data that is considered non-public data (DC-3 and DC-2) is covered by this policy. This includes information in any form (hard copy, electronic, or oral). The Department's Data Classification Table can be located at http://intranet/info-sec/data-class.html.

4.2. In the course of business, the Department receives, maintains, uses, and discloses confidential data relating to clients and Department staff. The Department shall maintain the confidentiality, availability, and integrity of all confidential data as required by all state and federal laws, and professional ethics.

4.3. This policy supplements, but does not replace any specialized training, policies, or procedures required by the Department's business areas to access non-public regulated confidential data (DC-3) and non-public restricted data (DC-2). It is expected that any business area handling DC-3 data shall promulgate additional policies and procedures for staff to follow based on the unique needs of the business area.

4.4. All data subject to a NH RSA 91-A Right to Know request shall be reviewed with the Department's Legal and Regulatory Services on a case-by-case basis prior to release.

4.5. Department staff shall safeguard all confidential data and shall only use, access, store, or disclose confidential data as necessary to perform their job related duties or assignments.

4.6. The Department has contracted data destruction services to securely destroy electronic and hard copy (paper/fax) data per Federal and State policy. It is the Department staff's responsibility to know and understand the data retention policy of the data they are handling. Non-public: regulated confidential, non-public: restricted, and public: non-published data shall have different data retention policies governing when the data may be legally destroyed. Prior to destroying non-public data (DC-3 and DC-2) consult with your business area's data steward for the data retention policy associated with said data.

4.6.1. Hard Copy: Public and non-public hard copy (paper or fax) data no longer required shall be placed in a Department bin designated for cross-shredding. Department staff shall not dispose of hard copy data by placing it in a recycling or trash receptacle.

4.6.2. Electronic Copy: The destruction of non-public electronic data shall follow DoIT policy located at: http://intranet/info-sec/policies.html, which adheres to Department of Defense (DOD data destruction standards. Electronic data includes but is not limited to hard drives, encrypted thumb drives, mobile devices, Secured Digital (SD) cards, and electronic devices with memory (which includes printers and scanners).

4.7. Department staff is legally and ethically obligated to maintain the confidentiality of Department client, patient, and other data classified as non-public data (DC-3 and DC-2) even after employment or agreement termination or privileged status expiration/termination.

4.8. Upon termination of employment or agreement or privileged status expiration/termination, the Department staff's access to NH State and Department systems, network, applications, subscriptions, social media accounts and other access related to the Department or the State of New Hampshire shall be terminated/revoked by the end of the business day of their last day of work/contracted obligation. If separation from the Department is unplanned, access shall be revoked immediately and deactivation complete prior to Department staff's departure. Former Department staff

shall not use, access, store or disclose any confidential data which was available to the former Department staff in the performance of his or her duties or assignment.

4.9. Non-public: regulated confidential, non-public: restricted, and public: non-published (DC-3, DC-2, DC-1) data in the possession or control of former Department staff at the time of or after termination shall be returned to the Department within 24-hours of termination.

4.10. Department staff or business areas shall receive approval from the data governance process prior to sharing/exchanging data outside of the Department or prior to sharing non-public regulated confidential data or non-Department data obtained through agreement. The sharing of data outside of the Department shall require a legal instrument, e.g., data sharing agreement (DSA), data exchange agreement (IEA), or a Memorandum of Understanding (MOU) executed by the Department's Commissioner or authorized designee.

4.11. Confidential data (DC-3 and DC-2 data) shall only be used in the performance of Department staff job duties or assignments. Department staff shall not remove, copy, transmit, or transfer materials or property containing confidential data from his/her business area unless it is necessary in the performance of their job duties and he/she has received written permission from their direct supervisor to remove materials and the supervisor has a documented list of materials leaving state premises. If materials or property containing confidential data are removed, copied, transmitted, or transferred from the Department, the Department staff shall safeguard the materials/property and control access as required by this policy, other Department policies, or state and federal law.

4.12. Any Department staff working via telework, remote desktop, or remote access shall safeguard and control access to all confidential data. Upon completion of any assignment or as requested by the Department staff's supervisor the Department staff shall secure all such materials/property and copies thereof or return all such materials/property and copies to the Department staff's supervisor. Contractors may be obligated to additional information security or business associate requirements.

4.13. Department staff or auditors shall not extract, print, print screen, scrape (hand copy information from screens), or photograph non-public regulated confidential data provided directly by federal agencies for any purpose, unless written exception is provided by the Department's Information Security Program and is supported by an executed Agreement with said Federal Agency.

4.14. Department staff shall not seek to access, use, or obtain any confidential data involving any matter which does not involve or relate to the Department staff person's specified or assigned job duties. Confidential data, Department records, documents, or other information shall not be maliciously tampered with, altered, or destroyed.

4.15. Department staff shall not seek to access, obtain, or use Department or confidential data for their personal use or for the use by family, friends, or acquaintances.

4.16. In the case of a health or safety emergency, relevant confidential data may be disclosed as necessary to appropriate individuals, e.g. police, a supervisor, or the Department's Information Security Program.

4.17. Each Department staff is responsible for completing Department annual information security, cybersecurity, privacy, and/or HIPAA trainings posted on the Department's Information Security intranet site prior to having access to or handling confidential data.

4.18. Each Department staff shall immediately report any known or suspected violations of this policy, or unauthorized use or access of confidential data by any means, to the DoIT Help Desk at helpdesk@doit.nh.gov. The process and guideline for reporting an Information Security or Privacy Event/Incident/Breach is located at: http://intranet/info-sec/reporting.html.

4.19. Prior to having access to or handling certain federal data all Department staff shall:

4.19.1 Complete a criminal records check as required by the Department's Criminal Records Check Policy and/or background check as required by the data's federal regulating agency's security policy.

4.19.2 Complete a criminal records check as required by the Department's Criminal Records Check Policy and/or background check as required by the data's federal regulating agency's security policy every five years.

- If the Bureau of Human Resources and the hiring authority determine that the returned criminal records check and/or background check adversely affects the Department staff's suitability for the position for which he/she holds, access to certain federal data shall be revoked and appropriate action shall be taken under the Administrative Rules of the Division of Personnel.

4.19.3 Receive a determination from the Bureau of Human Resources and the hiring authority that the criminal records check and/or background check condition of employment or agreement has been satisfied and the Department staff is suitable for the position for which he/she is being considered.

- Access to certain federal data shall be restricted until the Department has received and reviewed the results of the criminal records check and/or background check and a suitable determination has been received by the hiring authority.

4.19.4 Sign the Department's Business Use and Confidentiality Agreement, then sign it annually thereafter.

4.19.5 Complete the Department's mandatory secure email, information security, cybersecurity, privacy, and/or HIPAA training(s), then annually thereafter. Contractors

may have this requirement waived by providing signed attestation by their company's Human Resource Officer that the aforementioned training topics were successfully completed.

4.19.6 Contractors are required to provide the Department a signed attestation by their company's Human Resource Officer that they have had the required criminal records check and/or background check with acceptable results as required by the Department.

Section 5 - RESPONSIBILITY

5.1. The Bureau of Human Resource Management and the Bureau of Information Services, Information Security Program is responsible for developing, maintaining and monitoring this policy.

5.2. Department Directors, Administrators, and Supervisors are responsible for enforcing this policy.

5.3. Department staff are responsible for complying with this policy.

5.4. Human Resources shall perform an annual evaluation, review, and update of Department staff regulatory compliance trainings and provide a list by Division to the Division Directors for policy compliance.

5.5. Human Resources shall perform an annual review, and update of Department staff for background check regulatory compliance and provide a list by Division to the Division Directors of the Department staff requiring background checks.

Section 6 - SANCTIONS

6.1. Any Department employee found to have violated this policy shall be subject to appropriate discipline, up to and including termination, as provided by the Administrative Rules of the Division of Personnel.

6.2. Contractors, unpaid interns, and volunteers shall be subject to appropriate monitoring and compliance with this policy as provided by the contract or agreement with the Department.

Section 7 - DISTRIBUTION

7.1. Department policies are posted on the Department Intranet under the Policies and Procedures Section.

7.2. Human Resources shall notify all Department staff via e-mail when new policies are posted to the Intranet.

7.3. Supervisors responsible for Department staff that DO NOT have access to email shall bring this information to their attention as soon as possible.

7.4. Policies involving information security shall also be posted to the Department's website.