Data Classification, Handling, and Retention Policy

Revision History

Revision #	Date	Author	Sections Altered	Senior Management Approval
Rev 1.0	9/1/2012	Ben Price	New Document	
Rev 1.0	7/18/2013	Ben Price	None	
Rev 1.1	6/12/2014	Ben Price	Edited Retention	
Rev 1.2	11/2/2015	Ben Price	Edited Retention	
Rev 1.2	9/1/2016	Brad Carlton	Edited Full Backups and TOC	
Rev 1.2	09/05/2017	Jill Peden	Reviewed for Accuracy	
Rev 1.3	10/08/2018	Brad Carlton	Updated policy format. Removed TOC.	
Rev 1.4	12/29/19	Jill Peden	Annual Review for Accuracy	
Rev 1.5	06/08/2020	Brad Beeler-Carlton	Update to Policy, retention time from 2 years to 60 days	
-	06/07/2021	Brad Beeler-Carlton	Annual Review for Accuracy	
Rev 1.6	07/27/2022	Brad Beeler Carlton	Title Change and Policy Rewrite. All sections updated	
-	07/27/2023	Brad Beeler-Carlton	Annual Review for Accuracy	

Purpose

In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), L & D Mail Masters, Inc. is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), confidential, and sensitive information (hereafter referred to as data) it creates, receives, maintains, and/or transmits.

To comply with regulatory requirements, L & D Mail Masters, Inc. has established internal corporate governance for safeguarding the confidentiality, integrity, and availability of data the workforce creates, receives, maintains, or transmits. L & D Mail Masters, Inc. will have in place appropriate administrative, technical, and physical safeguards to protect data. It is the policy of L & D Mail Masters, Inc. to ensure that data is protected against misuse, loss, tampering, or use by unauthorized persons.

The purpose of this policy is to define L & D Mail Masters, Inc.'s data classification, handling procedures, and data retention regulations to ensure that the organization is properly safeguarding data in accordance with internal and regulatory requirements. The need to retain data varies widely with the type of data and the purpose for which it was collected. L & D Mail Masters, Inc. strives to ensure that data is only retained for the period necessary to fulfil the purpose for which it was collected and is fully deleted when no longer required.

Scope

This policy covers all data collected by L & D Mail Masters, Inc. and stored on L & D Mail Masters, Inc. owned or leased systems and media, regardless of location. It applies to both data collected and held electronically (including photographs, video, and audio recordings) and data that is collected and held as hard copy or paper files. The need to retain certain information may be mandated by federal or local law, federal regulations, and legitimate business purposes.

Responsibilities

Security Team Lead:

The Security Team Lead is responsible for working with senior management to assign classification labels to data handled by the organization. The classification labels must be reviewed periodically and updated when necessary. The Security Team Lead is also responsible for providing ongoing workforce education and awareness as it pertains to data classification and handling.

Senior Management:
Senior Management will provide support through active enforcement, funding, and resources needed to meet the requirements of this policy.

Workforce:

Workforce members are responsible for complying with this policy and reporting deviations and non-compliance to senior management. Workforce is defined as employees, trainees, and other persons who perform work for L & D Mail Masters, Inc.

Information Technology (IT) Department:

The IT Department at L & D Mail Masters, Inc. is responsible for the administration, configuration, and inventory, which includes content and location, of the organization's backups.

Third-Party Contractual Relationships:

Third parties performing work on behalf of L & D Mail Masters, Inc. that require them to have access to data will comply with this policy. L & D Mail Masters, Inc. personnel responsible for contractual oversight will ensure requirements of this policy are included in all contractual agreements to include a statement that non-compliance is grounds for contract termination.

Data Classification

All data created, processed, received, transmitted, and stored by L & D Mail Masters, Inc. workforce will fall under one of the following classifications:

- Public
- Protected
- Restricted
- Confidential

When the classification is unknown, the data must be classified as "Confidential."

Public:

Any data that can be given to the general public and can be distributed outside of L & D Mail Masters, Inc. without any risk, through various mediums. This is often general information about L & D Mail Masters, Inc. for marketing or product purposes.

Protected:

Data, which if disclosed, may cause the organization some financial, legal, or reputational damage. This data is typically used by workforce members during the standard course of business.

Restricted:

Data, which if disclosed, may cause the organization moderate financial, legal, or reputational damage. This data is typically reserved for business owners or senior management only.

Confidential:

Data, which if disclosed, is likely to cause the organization severe financial, legal, or reputational damage. This data typically includes protected health information (PHI) or employee personnel records.

PHI can be in the form of various media. Unauthorized disclosure could seriously and adversely impact L & D Mail Masters, Inc., and its clientele. Always obtain appropriate authorization for disclosures of PHI. A Business Associate Agreement (BAA) must be in effect for third parties to receive PHI.

Data Handling Methodology

PHI and other data will be stored in an encrypted format (encryption at rest). This includes data stored on servers, workstations, and other types of electronic media (e.g., laptops, tablets, smartphones, etc.). The minimum standard used for encryption will be 256 AES. If encryption is not possible or plausible, the Security Team Lead will perform a risk analysis to determine if the risk is acceptable and what additional controls will be needed. However, in the event that data is being stored in a non-secure area, then encryption is required with no exceptions allowed. Risk management activities will be performed in accordance with the organization's Risk Management policy. The same encryption standard will also be utilized for the transmission (e.g., SFTP, email, instant messaging, etc.) of data (encryption in transit).

L & D Mail Masters, Inc. will train workforce members on the appropriate systems and devices for the storage and transmission of data. This shall be technically enforced through system configuration in addition to training. However, L & D Mail Masters, Inc. will also ensure that the storage and transmission of data is kept to a minimum. Workforce members will also be trained in data handling procedures found in the organization's Clear Screen and Clean Desk Policy. Any workforce members found using an unapproved system or device for the storage or transmission of data will be considered non-compliant with this policy and be subject to disciplinary action.

Portable media containing PHI will be properly identified in a manner that individuals managing the media understand the sensitivity of the data stored on the device.

Portable media/devices containing PHI will be properly secured with encryption and physically safeguarded against theft, loss, and unauthorized access/modification when transferring outside of the organization and its facilities, to include in between facilities. All transfers of data outside of controlled areas will also require management approval.

In the event that mail services are utilized for the transport of PHI or other data, both internally and externally, it will be sent in a secure fashion.

Examples of protecting physical mail are:

- Authorized, trained personnel must oversee all mail.
- Clearly label with recipient's name and verify that address information is correct.
- Store all unattended mail in a closed, secure area.
- Place all types of media containing any form of PHI in secured, confidential envelopes and/or containers (internal and external).
- Return address on external mail consists of L & D Mail Masters, Inc. address only. There must be no mention of the contents.
- Opaque envelopes will be utilized for external mail and internal distribution of PHI to prevent viewing of information. Ensure that all envelopes are properly sealed (internal and external).

Data Backup Schedule

All end user or department data that is stored on the organization's internal network is automatically backed up and then replicated to an off-site location for a period of sixty (60) days. After the 60-day period, backups are automatically overwritten. Full backups are performed weekly, in addition to incremental backups being performed daily.

Backup Testing

Backups must be tested when any change is made that may affect the backup system. Backups must also be tested monthly to ensure the integrity of the backups in case of a crisis.

Data Retention

Data that is required to be kept for a specified length of time, either by regulatory requirements or contractual agreements, will adhere to the following retention schedule:

- Current employee personnel folders, 401(k) plan records, certificates of tax exemption, state and county assessments, state and county tax bills, federal and state income tax returns, audit reports, and corporate minutes will be kept indefinitely.
- Employee earnings records, former employee personnel folders, payroll time sheets, payroll journals, wage rate changes, vendor invoices, client invoices, sales contracts, sales and use tax returns, unemployment tax returns, withholding tax returns, company notices, notice acknowledgements, restrictions in writing, and bank statements and reconciliations will be kept for a period of ten (10) years.
- OIG and SAM (GSA) Screening evidence for each employee prior to hire and monthly thereafter and the employee roster subject to each monthly screening, will be kept for a period of 10 years.
- Training records or documentation for HIPAA, General Compliance and Fraud, Waste and Abuse Training, Standards of Conduct Training, and Compliance Policy Training that include employee name and date completed, will be kept for a period of 10 years.
- Documentation pertaining to any suspected or confirmed Fraud, Waste and Abuse issues, and/or compliance related issues, will be kept for a period of 10 years.

- All records and documentation related to disclosures of data, including the information required for disclosure, the written account provided to the individual, and the L & D Mail Masters, Inc. workforce member involved will be retained for a period of 10 years.
- All formal policies and procedures and other critical records will be retained for a period of 10 years.

Data Destruction

L & D Mail Masters, Inc. manages the data it controls, and processes it in an efficient and responsible manner. When the retention period for the data as outlined above expires, L & D Mail Masters, Inc. must actively destroy the data covered by this policy. If an individual feels that certain data should not be destroyed, they should identify the data to the IT Department at L & D Mail Masters, Inc. so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by the President of L & D Mail Masters, Inc.

The disposal of non-electronic media (e.g., hard drives) will be handled by an industry approved destruction method. See L & D Mail Masters, Inc.'s Media Reuse and Secure Disposal Policy for more information on the approved destruction method.

Enforcement

This policy will be enforced by the company's Security Team Lead. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company may report such activities to the applicable authorities. The company reviews this policy annually for improvement opportunities and reserves the right to revise this policy at any time.