



Moving Information Forward

HIPAA
Policy and Procedure Manual

Table of Contents

HIPAA TERMS	1
GENERAL POLICY ON PROTECTED HEALTH INFORMATION.....	4
REGULATORY COMPLIANCE PROGRAM.....	5
USE AND REPORTING OF PRIVATE HEALTH INFORMATION	6
CONFIDENTIALITY AND BUSINESS ASSOCIATE AGREEMENTS	8
DATA INTEGRITY	10
REQUEST FOR ACCOUNTING	11
MITIGATION OF UNAUTHORIZED DISCLOSURES	12
REPORTING PROBLEMS AND VIOLATIONS	13
INFORMATION PRIVACY AND SECURITY TRAINING	14
TERMINATION OF EMPLOYMENT	15
RECEIPT OF DATA	16
PHYSICAL ACCESS CONTROL.....	17
NETWORK ACCESS	19
DATA ACCESS	20
REMOTE ACCESS	21
BACKUP AND RECOVERY	22
STORAGE AND DESTRUCTION.....	24

HIPAA TERMS

DASHER Inc.'s Health Insurance Portability and Accountability Act ("HIPAA") Policy and Procedure Manual is designed with the intent of meeting the terms identified in 45 CFR 160.103 and 164.501, as noted below:

Business associate: (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

- (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Covered entity means:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered



Moving Information Forward

entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- (1) Investigate or conduct an official inquiry into a potential violation of law; or
- (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of electronic media at 162.103 of this subchapter; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv). Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or



Moving Information Forward

analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Required by law means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law.

Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.



Moving Information Forward

PROTECTED HEALTH INFORMATION
PRIVACY, SECURITY AND CONFIDENTIALITY

POLICY

It is the policy of DASHER Incorporated (DASHER) to use appropriate safeguards to prevent inappropriate use or disclosure of Protected Health Information (PHI). DASHER will make all efforts to protect individually identifiable health data so that disclosure of such data will be at the minimum necessary extent needed to administer healthcare operations as required by law.

PURPOSE

In the course of normal business operations, DASHER recognizes that it may be entrusted with PHI. DASHER further recognizes its ethical and legal obligations to protect and ensure the privacy, security and integrity of PHI to the fullest reasonable extent.

Our responsibilities to protect PHI encompass protection not only of data and information but also facilities, equipment and media in which confidential information may be stored or processed. DASHER shall ensure that its policies and procedures meet or exceed the standards set by state and federal law for privacy protection of PHI and adhere to any related provisions within agreements with business associates.

REGULATORY COMPLIANCE PROGRAM

POLICY

It is the policy of DASHER Incorporated (DASHER) to remain in compliance with all federal and state regulatory statutes by protecting the confidentiality and security of Protected Health Information (PHI).

PURPOSE

The purpose of this policy is to ensure DASHER's awareness and compliance with identified and applicable laws regarding the access, use, distribution and housing of PHI. In the course of normal business operations, DASHER recognizes that it may be entrusted with PHI. DASHER will protect and ensure the privacy, security and integrity of PHI to the fullest reasonable extent.

PROCEDURE

For each jurisdiction where DASHER conducts operations using PHI, DASHER will:

1. Research each jurisdiction's laws and regulations to identify any relevant statutes applicable to protecting the confidentiality and security of PHI.
2. Consult with legal counsel to obtain clarification, when necessary, of the jurisdiction's laws and regulations.
3. Compare DASHER's policies and procedures for protecting PHI to each jurisdiction's applicable laws and regulations to:
 - A. Identify any discrepancies between DASHER's current policies and procedures with the jurisdiction's legal requirements.
 - B. Provide documentation on statutory discrepancies to the project director and/or DASHER senior management.
 - C. Have project director and/or DASHER senior management evaluate the need to change policies and procedures.
 - D. Obtain the required signatures and sign-offs as necessary.
4. Place any relevant documentation into a central file or binder and make available to DASHER staff.
5. Educate involved staff on changes to policies and procedures.
6. Monitor on an ongoing basis any new regulatory requirements, and repeat procedure 1 to 5, as needed.

Last revised: December 22, 2010



Moving Information Forward

USE AND REPORTING OF PROTECTED HEALTH INFORMATION

POLICY

It is the policy of DASHER Incorporated (DASHER) to ensure that all analytical output and reports based on Protected Health Information (PHI) conform to DASHER's business associate agreement and/or client contract. DASHER will only report individually identifiable information when such reporting does not violate state or federal laws.

DASHER shall not disclose PHI that may reasonably permit the identification of an identified individual to a third party except as necessary to (1) agents with whom the appropriate business associate agreements have been obtained or (2) pursuant to a release or court order. The party making the disclosure shall ensure that any release relied upon for these purposes is (a) in written form, with a copy retained in the records of the disclosing party, (b) executed by a person with the legal authority to enter into such a release, (c) legally applicable to the information to be disclosed, and (d) effective on the date of disclosure.

PURPOSE

The purpose of this policy is to ensure that PHI is used and reported in a manner consistent with DASHER's business associate agreement/client contracts and statutory requirements. This will assist in preventing unauthorized use and disclosure of PHI.

PROCEDURE

1. Employees shall adhere to the business associate agreement/client contract in regard to appropriate uses and disclosures (i.e. reporting) of PHI – See CONFIDENTIALITY AND BUSINESS ASSOCIATE AGREEMENTS
2. All staff involved with a particular client contract shall be informed of appropriate uses or disclosures of PHI under the client contract and the Privacy Rule.
3. Only DASHER staff involved in specified client work will have access to PHI.
4. PHI shall be used and reported in the minimum amount necessary to meet the intended purpose of the business associate agreement/client contract.
5. Information containing PHI will only be shared with those entities with authority to receive such information as (a) defined by signed confidentiality and/or business associate agreements, and (b) allowed by federal and state law.



Moving Information Forward

6. When information containing PHI is sent to an individual (i.e. independent reviewer) or other authorized entity with whom DASHER maintains a signed confidentiality and/or business associate agreement, DASHER staff will:
 - Maintain a copy of the information being sent in a secure location (i.e. locked file drawer or cabinet)
 - Remind entity of the confidential nature of the information being sent
 - Request return to DASHER of all information, including notes and copies, at the completion of the service for proper disposal by DASHER staff
 - Document the following information:
 - a. Description of the information being sent
 - b. Date information was sent
 - c. Date the information was returned in its entirety
7. Reports and other information that discloses PHI should be aggregated to the maximum extent possible that also achieves the requirements by the client. PHI shall be reported at the individual level only if required, as documented in the client contract and/or business associate agreement.
8. DASHER staff shall document verbal client requests for reports containing PHI.
9. DASHER staff shall document verbal client requests for reports containing PHI to be delivered by e-mail.
10. E-mail shall not be utilized to deliver PHI or client confidential materials unless (a) permission is granted by the client, and (b) security measures are in place for the transmittal of such data.
11. Reports shall be delivered by trackable mail, such as FedEx.
12. All outgoing reports and information containing PHI shall be sealed, addressed to an authorized recipient and clearly marked as confidential.
13. DASHER shall consult with legal counsel, as necessary, to determine whether certain uses or disclosures of PHI are permissible.

Last revised: December 22, 2010



Moving Information Forward

CONFIDENTIALITY AND BUSINESS ASSOCIATE AGREEMENTS

POLICY

It is the policy of DASHER Incorporated (DASHER) to enter into confidentiality and/or, business associate agreements, as required, with employees, independent contractors, clients and other parties involved in the acquisition and analysis of client data that involves Protected Health Information (PHI). Furthermore, it is DASHER's policy that these agreements and DASHER's client contracts shall identify individual and organizational responsibilities; appropriate usage of data and reports; and persons authorized to release and receive PHI, as well as other jointly defined parameters.

PURPOSE

DASHER's PHI confidentiality and security program safeguards the interests of DASHER, its clients, the clients' data suppliers, and the individuals who are the original source of data. Confidentiality and business associate agreements provide the guidelines for appropriate behavior at both the individual and organizational levels, in addition to state and federal laws.

PROCEDURE

1. Upon employment, DASHER staff shall sign confidentiality agreements, which provide general guidelines for the appropriate use and disclosure of PHI and any uses thereof.
2. Depending on the nature of the engagement and the requests by DASHER's client, DASHER may require staff to enter into separate confidentiality agreements for a specified engagement or project. These client specific confidentiality agreements shall identify the appropriate use and disclosure of PHI by DASHER staff.
3. DASHER shall enter into confidentiality and/or business associate agreements with clients, as requested, for engagements involving PHI. These agreements may include:
 - a. Appropriate and planned use of PHI
 - b. Authorized persons to accept and provide PHI
 - c. Reports to be prepared, including permission to provide patient level reports if required
 - d. Report delivery method
 - e. Agreement to use PHI only for contracted purpose
 - f. Method of disposal of PHI at end of project, if required



4. DASHER shall require independent contractors and other entities that may require or come into contact with PHI, to sign confidentiality and/or business associate agreements and to comply with the client contract and/or business associate agreements under which DASHER has contracted them.
5. DASHER shall not use or disclose PHI except as permitted by the client agreement or as required by law.

Last revised: December 22, 2010



Moving Information Forward

DATA INTEGRITY

POLICY

It is the policy of DASHER Incorporated (DASHER) to not change or modify any original data that includes Protected Health Information (PHI) provided by clients/business associates, unless requested by client. It is the policy of DASHER to only make amendments to PHI that is directed by the client, as long as this does not violate state or federal law.

PURPOSE

The purpose of this policy is to ensure and maintain data integrity, which is critical for reliable and valid analysis. Data sources (clients, business associates, etc.) are ultimately responsible for the contents of the data provided.

PROCEDURE

All Services:

- DASHER employees shall never change or alter original data containing PHI, unless the client directs such amendments in writing. A copy of the written directive shall be maintained with the relevant data file.

Data Analysis Services:

- Where data containing PHI needs to be recoded or manipulated, DASHER employees will add new field/columns to data tables so that the original data is maintained.
- DASHER employees shall keep the original copy of raw data containing PHI available in case of hardware/software failure or to ensure data integrity.

Last revised: December 22, 2010



Moving Information Forward

REQUEST FOR ACCOUNTING

POLICY

It is the policy of DASHER Incorporated (DASHER) to provide business associates/clients a timely accounting of disclosures of Protected Health Information (PHI), upon request.

PURPOSE

The purpose of this policy is to ensure that all requests for PHI disclosures for which individuals have a right to request an accounting by business associates/clients can be met in a timely manner.

PROCEDURE

1. Upon request, DASHER will make available to client reports relating to the use and disclosure of PHI for which individuals have a right to an accounting.
2. DASHER shall provide the report(s) in a timely manner.

Last revised: December 22, 2010



Moving Information Forward

MITIGATION OF UNAUTHORIZED DISCLOSURES

POLICY

It is the policy of DASHER Incorporated (DASHER) to mitigate, to the extent practicable, any harmful effect that is known to DASHER of a use or disclosure of PHI by DASHER in violation of the requirements of the business associate/client agreement. DASHER will put forth its utmost efforts to ensure that PHI is not used outside of the contractual terms agreed to with the client.

PURPOSE

While DASHER safeguards confidential client information, including PHI, to the fullest extent possible, there remains the possibility that confidential client information/PHI, may be disclosed unintentionally and/or used inappropriately. In such instances, DASHER will mitigate, to a reasonable extent, any documented harmful effects.

PROCEDURE

1. DASHER employees shall document any disclosure of PHI not authorized by the business associate/client agreement and investigate the circumstances of the disclosure.
2. DASHER shall document any harmful effects and/or request documentation of harmful effects from the involved parties.
3. DASHER shall develop a mitigation plan with harmed parties and implement that plan.
4. DASHER shall review the circumstances that permitted the disclosure and alter policies and procedures to prevent re-occurrence.
5. Sanctions (to include termination of employment in appropriate circumstances) will be imposed upon employees or independent contractors found to have violated DASHER's policies.

Last revised: December 22, 2010



Moving Information Forward

REPORTING PROBLEMS AND VIOLATIONS

POLICY

It is the policy of DASHER Incorporated (DASHER) to encourage all employees who believe that a breach of the privacy and/or security of Protected Health Information (PHI) has occurred or reasonably believe that a breach may occur, to report their concerns to the appropriate DASHER staff person.

It is also the policy of DASHER to report to the client any known uses or disclosures of PHI that is not authorized in the business associate/client agreement.

PURPOSE

The purpose of this policy is to encourage all staff to be vigilant in guarding confidential client data, especially data containing PHI. Staff working with client data/PHI often have the best perspective to identify potential confidentiality and security lapses and may be the first to discover any unauthorized disclosure or inappropriate use of PHI.

It is also the purpose of this policy to assure that any unauthorized disclosures of PHI will be reported to the business associate/client.

PROCEDURES

- Employees who have a reasonable basis to believe that a breach of confidentiality has occurred should report the incident as soon as possible to any of the following:
 - Immediate Supervisor
 - HIPAA Compliance Officer
 - President and Chief Operating Officer
- Employees who have a reasonable basis to believe that a breach of confidentiality has occurred but does not report the event may be subject to corrective action, up to and including termination.
- DASHER shall report all known unauthorized uses and disclosures of PHI to the applicable client.

Last revised: December 22, 2010



Moving Information Forward

INFORMATION PRIVACY AND SECURITY TRAINING

POLICY

It is the policy of DASHER Incorporated (DASHER) to provide privacy and security awareness training regarding Protected Health Information (PHI) to new employees and additional training and/or reminders to existing employees as necessary.

PURPOSE

DASHER wants to make all employees aware of their responsibility to keep secure and confidential all sensitive client data, especially data containing PHI, through training and/or periodic reminders.

PROCEDURE

1. Privacy and security awareness training topics will include, but are not limited to, procedures delineated under the HIPAA Policies and Procedures Manual.
2. All new employees shall be required to read the HIPAA Policies and Procedures Manual within 30 days of employment or prior to having access to PHI, whichever occurs sooner.
3. All DASHER employees shall be required to attend privacy and security awareness training prior to having access to PHI.
4. All DASHER staff shall be required to attend privacy and security awareness training at least annually as well as receive training through periodic security reminders to be distributed as warranted.

Last revised: December 22, 2010



Moving Information Forward

TERMINATION OF EMPLOYMENT

POLICY

It is the policy of DASHER Incorporated (DASHER) to minimize access to confidential client data, including Private Health Information (PHI), by terminated staff members.

PURPOSE

The purpose of this policy is to ensure that access to PHI by staff members whose employment is terminated is minimized.

PROCEDURE

Upon termination of employment of a staff member, the following will occur:

1. DASHER will remove access, including remote access if available, to the local area network, particularly computer drives housing client data with PHI.
2. Passwords for terminated employees will be changed.
3. Keys needed to obtain access to the building after hours will be collected from the terminated employee.

Last revised: December 22, 2010



Moving Information Forward

RECEIPT OF DATA

POLICY

It is the policy of DASHER Incorporated (DASHER) to keep a log of all client data containing Protected Health Information (PHI) that is submitted to DASHER.

PURPOSE

The purpose of this policy is to have a record of all client data received by DASHER that includes PHI. These records shall be easily searched so that the receipt of data can be easily confirmed.

PROCEDURE

Upon receipt of client data containing PHI, a designated DASHER employee (whose identity may vary based on the client and/or service line) shall maintain a log of the data received. The data shall include:

1. Date received,
2. File name or description of information received,
3. Format (hard copy versus electronic), and
4. Date copied to network upon receipt of data, if applicable.

DASHER staff will request that any entity sending information that may contain PHI via facsimile use DASHER's secure and confidential fax line, if applicable.

Last revised: December 22, 2010



Moving Information Forward

PHYSICAL ACCESS CONTROL

POLICY

It is the policy of DASHER Incorporated (DASHER) to limit physical access to its office space and equipment to authorized persons.

PURPOSE

The purpose of this policy is to prevent unauthorized persons from accessing DASHER office space and equipment. Unauthorized persons who gain access to DASHER's office space and equipment may also attempt to access DASHER's computer network. The NETWORK ACCESS and DATA ACCESS policies further protect PHI from unauthorized access.

PROCEDURE

Access to building and DASHER offices shall be restricted, as follows:

1. Visitors shall register with the receptionist upon entering the building and be required to wear a "visitor" badge.
2. A DASHER employee shall accompany DASHER visitors from the receptionist area to the DASHER offices.
3. Employees shall be required to show their photo identification badge and sign-in with the security guard after regular hours in order to gain access to the building.
4. Visitors shall not be given access to PHI, either on the DASHER network or hard copy, unless they are duly authorized (i.e. a client, business associate). Access in such instances shall be limited to the PHI which the visitor is authorized to access.
5. When the building is closed with no security guard on duty, the building shall be armed and monitored by ADT Security Systems

Access to PHI shall be restricted, as follows:

1. Only authorized staff members shall be given access to PHI
2. DASHER employees shall not leave PHI on their desk or other accessible workspace when the employee is not in the area for extended periods of time.
3. DASHER employees shall lock PHI in file cabinets or secure rooms after business hours.
4. DASHER employees shall keep CDs and other media sent to DASHER containing PHI in a secured area.
5. DASHER employees shall restrict removal of PHI from DASHER premises to only authorized staff, contracted business associates and/or clients.



6. When PHI is removed from the premises, DASHER employees shall secure PHI either (1) in a sealed envelope that is clearly marked confidential or (2) in a locked briefcase for transportation.
7. When DASHHER employees anticipate receipt of data containing PHI, DASHHER employees shall identify for the client the staff member's name to whom the confidential information should be sent.
8. When DASHHER employees anticipate the receipt of data containing PHI via facsimile, DASHHER employee shall provide the client and/or business associate with the secure and confidential fax number.
9. See NETWORK ACCESS and DATA ACCESS policies for additional security information related to DASHHER's computer network and files

Last revised: December 22, 2010



Moving Information Forward

NETWORK ACCESS

POLICY

It is the policy of DASHER Incorporated (DASHER) to limit access to its computer network to authorized persons.

PURPOSE

The purpose of this policy is to prevent unauthorized persons from accessing DASHER's computer network. Unauthorized persons with access to DASHER office space and equipment may also attempt to access the computer network. This policy prevents unauthorized persons from accessing DASHER's computer network either intentionally or unintentionally. The DATA ACCESS policy further protects Protected Health Information (PHI) from unauthorized access.

PROCEDURE

1. DASHER's server shall be maintained in a secure area which shall be locked after normal business hours.
2. A username and password shall be required to gain access to the network.
3. Only authorized employees shall have access to (a) location of the server key, and (b) the username and password to DASHER's server.
4. Each employee will be assigned his/her own individual username and password to gain access to the network.
5. Network password must be changed periodically, cannot be reused and shall not be shared with other employees.
6. See DATA ACCESS policy for additional security issues related to passwords.
7. Access to the network shall be denied after a specified number of invalid attempts.
8. Rights to PHI on DASHER's network will be limited via drive accessibility. Only those with a need to use PHI data to perform client services will have logon/passwords that provide access to drives on the network that are designated for PHI.
9. Visitors shall not be given access to the DASHER network and PHI without permission from a member of the DASHER management team. Appropriate safeguards shall be employed in these instances to limit access to only the PHI which the visitor is authorized to access.
10. Employees should not leave computers unattended with PHI on screen.
11. Screen savers that are password protected should be utilized to assist as a protective device in the event that PHI is left unintentionally on screen.

Last revised: December 22, 2010



Moving Information Forward

DATA ACCESS

POLICY

It is the policy of DASHER Incorporated (DASHER) to limit access to client data containing Protected Health Information (PHI) to authorized persons only.

PURPOSE

The purpose of this policy is to prevent unauthorized persons from accessing DASHER's client data that includes PHI. Unauthorized persons who gain access to DASHER's computer network may also attempt to access client data and/or PHI either intentionally or unintentionally. This policy prevents persons with access to DASHER's computer network from accessing client data/PHI.

PROCEDURE

1. All computer terminal access, including portable laptop computers, should be controlled through a username and password. See NETWORK ACCESS policy for additional information related to network access controls.
2. Passwords shall be selected and maintained by the individual users.
3. Passwords should be at least six characters long, not involve personal or obtainable information, nor be used repeatedly.
4. Users shall select and change their own passwords, and will be prompted on a regular basis to do so.
5. Users shall not share passwords.
6. Users shall not write down passwords, store them on hard copy or keep them on a personal computer for remote log-on purposes.
7. Rights to PHI on DASHER's network will be limited via drive accessibility. Only those with a need to use PHI data to perform client services will have logon/passwords that provide access to drives on the network that are designated for PHI.
8. All databases with PHI shall be logon/password protected.
9. Employees who are issued personal digital assistants (PDA's) shall lock access to the device using individual user passwords.

Last revised: December 22, 2010



Moving Information Forward

REMOTE ACCESS

POLICY

It is the policy of DASHER Incorporated (DASHER) to limit remote access to client data containing Protected Health Information (PHI) to authorized persons only. Remote access will only be granted under agreement of all parties and shall be included in client contracts and/or business associate agreements. When remote access is granted, appropriate security measures will be utilized.

PURPOSE

The purpose of this policy is to eliminate the potential for confidential data containing PHI to be inappropriately disclosed or copied via remote access. By requiring that all parties agree to remote access, DASHER makes clients aware of any security issues related to remote access.

PROCEDURE

1. DASHER shall authorize employees to gain remote access via modem through an approved security device such as a dial-back system or hardware token technology.
2. If a security device is not used for remote access, a DASHER employee shall enable and disable the modem and directly supervise its use. This employee shall not leave the modem unattended in answer mode.
3. The same network access and data access procedure (identified in Policy #13 and #14, respectively) shall apply to remote access of PHI.

Last revised: December 22, 2010



Moving Information Forward

BACKUP AND RECOVERY

POLICY

It is the policy of DASHER Incorporated (DASHER) to backup computer files on a regular basis. This includes client data containing Protected Health Information (PHI). Backup tapes shall be kept available to recover any “lost” data due to computer/network failure, natural disasters, etc. Periodically, backup tapes will be stored offsite in a secure location to ensure that a copy of client data, including PHI, exists in the case of computer/network failure, natural disasters, etc. that could destroy all copies of client data/PHI onsite at DASHER.

PURPOSE

The purpose of this policy is to ensure that all client data/PHI is recoverable in the case of computer/network failure, natural disasters, etc. Furthermore, this policy ensures that DASHER will be able to continue its business functions in the case of loss of data due to computer/network failure, natural disasters, etc.

PROCEDURE

Backup

1. Multiple levels of backup and storage should be used for key data and files.
2. A daily backup of critical computer files shall be performed and stored in the server cubicle.
3. A weekly backup of all network drives shall be performed and sent off site and stored until the following week.
4. A monthly backup of critical files shall be performed and stored on-site in a fireproof, permanent storage vault.
5. Users of personal computers are responsible for the backup and recovery of their system files and programs. Files containing PHI shall not be stored on C: drives.
6. Files and programs on the network shall be properly labeled and indexed to facilitate recovery.



Disaster Plan

1. The individual who first discovers a disaster situation will immediately report the condition/ event to DASHER's President and COO or, if unavailable, their supervisor.
2. DASHER's President and COO will direct assigned tasks based on the nature and extent of the situation.
3. In the event of a computer failure, computer support services will be notified and a designated employee will obtain the most recent backup data for reinstallation. If computers and/or the network are destroyed, a person or team of individuals will be assigned to arrange for replacement of the equipment as quickly as possible.
4. In the event that DASHER's offices are destroyed, employees will report to work at the specified location.

Employees will follow the disaster recovery plan defined in the Independent Review Organization's policies and procedures. This comprehensive recovery plan includes specifics related to the disaster recovery process, team alert list, employee call list as well as other important steps.

Last revised: December 22, 2010



Moving Information Forward

STORAGE AND DESTRUCTION

POLICY

It is the policy of DASHER Incorporated (DASHER) to maintain final reports in a secure area and to properly destroy all other information containing Protected Health Information (PHI) in a manner that prevents unauthorized access to PHI.

PURPOSE

The purpose of this policy is to ensure that all documents containing PHI are either stored in a secure area or are disposed of in a manner to prevent the unauthorized access to such sensitive information.

PROCEDURE

Written or Paper Copies:

1. DASHER employees shall maintain all notes related to the final client work in a secure location.
2. Copies of final reports shall be kept in reasonably secure areas in DASHER offices.
3. Final reports containing PHI shall be kept in locked files and maintained for a period of time that is consistent with the Business Associate Agreement, if specified, or DASHER's record retention policy.
4. DASHER employees shall either shred or place all paper reports and/or work product containing PHI to be destroyed in the locked, grey disposal containers identified for shredding. This shredding requirement includes any work containing PHI which is generated at a remote location or removed from DASHER's premises. If shredding capabilities are not available at the remote location, DASHER employees shall transport work containing PHI to DASHER's offices for proper destruction. (See PHYSICAL ACCESS CONTROL). No reports containing PHI should be placed in regular garbage cans for disposal.



Electronic Copies:

1. DASHER employees shall maintain all data containing PHI on a network drive with access restricted to only authorized staff members.
2. If data containing PHI is received or stored on a CD, diskette or tape, DASHER staff shall maintain these items in a locked area with access restricted to only authorized staff when they are not in use.
3. DASHER staff will clear all CD's, diskettes and tapes containing PHI prior to disposing of these items.
4. With the exception of laptops, DASHER staff will not save files containing PHI to their C: drive. For laptops, DASHER staff will save PHI to the C: drive on a temporary basis and only with the appropriate use of logon passwords **and** unique file passwords. Files containing PHI will be moved to the network drive with restricted access upon return to the DASHER offices and will not be stored indefinitely on the C: drive of laptops.
5. Prior to disposal of personal computers, DASHER staff will request that the computer support services erase any stored files on the C: drive to assure files containing PHI were not inadvertently saved to the C: drive.

If it is not feasible to destroy either the written or electronic files, DASHER staff will continue to safeguard PHI from unauthorized access.

Last revised: December 22, 2010



Moving Information Forward