NFP HIPAA HANDBOOK

NFP HIPAA HANDBOOK

Table of Contents

General HIPAA Compliance for BAs Policy 101 1
HIPAA Policies & Procedures Maintenance Policy for Business Associates 102 3
HIPAA Documentation Policy for Business Associates 103 4
HIPAA Investigation Policy 104 6
Breach Notification Policy 105 9
Privacy Officer Policy 106 12
HIPAA Training Policy 107 14
PHI Uses and Disclosures Policy 108 15
PHI Patients' Rights Policy 109 19
Privacy Complaints Policy 110 23
Risk Management Policy 111 25
Sanctions Policy 112 27
Assignment of Security Responsibility Policy 113 28
Workforce Clearance Policy 114 29
Access Termination Policy 115 30
Access Authorization Policy 116 31
Access Establishment & Modification Policy 117 33
Security Awareness and Training 118 35
Policy for BAs on Security Incident Procedures 119 37
Data Backup & Storage Policy 120 39
Disaster Recovery Policy 121 40
Emergency Mode Operations Policy 122 42
Policy on Testing & Revision of Contingency & Emergency Plans 123 45
Policy on Data & Applications Criticality Analyses 124 46
Policy on Evaluating the Effectiveness of Security Policies 125 48
NFP Business Associates Policy 126 49
Facility Access Control Policy 127 51
Workstation Use and Security Policy 128 53
Media Disposal and Re-Use Policy 129 55
Access Control Policy 130 57
Audit Controls Policy 131 60
Data Integrity Controls Policy 132 61
Person or Entity Authentication Policy 133 63
Data Transmission Security Policy 134 65
Mobile Device Policy 135 66

COMMONLY USED ACRONYMS

Business Associate **(BA)**

Business Continuity Plan **(BCP)** Chief Compliance Officer **(CCO)**

Chief Privacy Officer **(CPO)**

Chief Technology Officer **(CTO)**

Coordinated Incident Response Team **(CIRT)**

Cyber-Security Incident Response Plan **(CSIRP)**

Department of Health and Human Services **(HHS)**

Designated Record Set **(DRS)**

Electronic PHI **(EPHI)**

Health Insurance Portability and Accountability Act **(HIPAA)**

Health Information Technology for Economic and Clinical Health **(HITECH)** Act of 2009

Individually Identifiable Health Information **(IIHI)**

National Institute for Standards and Technology **(NIST)**

NFP Corp. **(NFP)**

Office for Civil Rights **(OCR)**

Protected Health Information **(PHI)**

Self-Regulatory Organization **(SRO)**

U.S. Department of Health and Human Services **(HHS)**

Policy Number: 101
Date of Adoption:
Date of Review/Revision:

GENERAL HIPAA COMPLIANCE FOR BUSINESS ASSOCIATES POLICY

Introduction

Covered entities (and group health plan sponsors) that need assistance in performing plan administrative functions will likely hire outside entities or parties to perform specific plan functions. These entities are known as "business associates" (BAs) of the covered entity. NFP Corp. (NFP) is a BA and has adopted these HIPAA policies and procedures for BAs (No. 101 through 135) in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act) and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). The HITECH Act of 2009 made the portions of the HIPAA Privacy and Security Rules directly applicable to BAs. As applicable, officers, agents, employees, BAs, contractors, temporary workers, and volunteers must read, understand, and comply with the NFP's HIPAA policies and procedures in full and at all times.

NFP acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information (IIHI) generally, and Protected Health Information (PHI) as defined in the HIPAA Privacy and Security Rules, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. NFP also acknowledges our responsibility to facilitate the flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs General HIPAA Compliance for NFP, its subsidiaries and affiliates (together referred to in these policies as NFP) that handle IIHI, including PHI. Note that PHI is a subset of IIHI, which generally becomes PHI when a covered entity or BA of a covered entity creates, receives or maintains the information. All NFP workforce members, which hereafter includes independent contractors, agents and principals, must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

NFP recognizes that certain subsidiaries and affiliates of NFP constitute a BA under the definitions contained in the HIPAA rules. NFP must comply with HIPAA and the HIPAA Privacy and Security Rules, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended. Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity. Additionally, compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts. Finally, compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of PHI, and reduces the risk of breaches of confidential health data.

Policy Statement

NFP's policy is to become and to remain in full compliance with all the applicable requirements of HIPAA. Additionally, NFP's policy is to document HIPAA compliance-related activities and efforts as required by law. HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later.

Procedures

In accordance with the HIPAA Privacy and Security Rules, NFP commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

- **Privacy Policies and Procedures –** NFP will develop and implement written privacy policies and procedures that are consistent with the HIPAA Privacy and Security Rules.

- **Privacy Personnel –** NFP will designate a Chief Privacy Officer (CPO) responsible for developing and implementing NFP's privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on NFP's privacy practices. NFP's CPO will designate as many local HIPAA privacy officers as necessary. The local HIPAA privacy officers will report to the CPO and assist the CPO in the implementation, enforcement and maintenance of NFP's privacy policies and procedures.
- **Workforce Training and Management –** Workforce members include employees and may also include other persons whose conduct is under the direct control of NFP (whether or not they are paid by NFP). NFP will train all workforce members whose responsibilities include the handling of PHI on HIPAA requirements.
- **Sanctions –** NFP will have and apply appropriate sanctions against workforce members who violate NFP's privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
- **Mitigation –** NFP will mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its workforce or its BAs in violation of NFP's privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
- **Data Safeguards –** NFP will maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of PHI in violation of NFP's privacy policies and procedures, and/or HIPAA's Privacy and Security Rules, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.
- **Complaints –** NFP will develop procedures for individuals to complain about NFP's compliance with its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
- **Retaliation and Waiver –** NFP will not retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. NFP will not require an individual to waive any right under HIPAA's Privacy and Security Rules as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.
- **Documentation and Record Retention –** NFP will maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints (upon creation of a complaint mechanism), and other actions, activities, and designations that the HIPAA Privacy and Security Rules require to be documented.
- **Compliance and Enforcement –** NFP managers and supervisors are responsible for enforcing this policy. Employees who violate NFP's privacy policies and procedures, and/or HIPAA's Privacy and Security Rules, are subject to discipline up to and including termination in accordance with NFP's Sanctions Policy.

FAQ

Question: What does the HIPAA Privacy Rule do?

Answer: The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other personal health information. In addition, the HIPAA Privacy Rule:

- Gives individuals more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- Holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- Strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

Policy Number: 102
Date of Adoption:
Date of Review/Revision:

HIPAA POLICIES AND PROCEDURES MAINTENANCE POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs HIPAA Policies and Procedures Maintenance for BAs of NFP that handle IIHI and PHI. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to create and implement appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics. All NFP policies and procedures will be updated and amended as needed or as required by law. Moreover, all NFP policies and procedures will be distributed to, or made otherwise available to, the applicable workforce in a manner to be determined. Finally, NFP policies and procedures will be regularly maintained and secured, and copies will be stored with other important business records for safekeeping.

All NFP workforce members who handle IIHI and PHI in the normal course of their work functions are required to read, understand and comply with NFP's HIPAA policies and procedures.

Procedures

NFP will create or revise its own HIPAA policies and procedures, consistent with all applicable HIPAA Privacy and Security Rules and Regulations as they pertain to BAs. NFP will designate a qualified individual to assume control of the policies and procedures process. This individual will be called the CPO and will execute the creation or revision process in a timely manner. NFP will internally publish its HIPAA policies and procedures (when complete) to its subsidiaries and affiliates that act as a BA or otherwise handle PHI. NFP will provide access to all applicable workforce members and will provide appropriate training to members of its workforce on the interpretation and implementation of its policies and procedures.

FAQ

Question: Who must comply with HIPAA privacy standards?

Answer: The Privacy Rule covers: Health plans (e.g., health insurance companies, company health plans, government programs that pay for health care); Health care clearinghouses (i.e., entities that process nonstandard health information they receive from another entity into a standard); and Health care providers (e.g., doctors, clinics, pharmacies) who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted under HIPAA, such as electronic billing and fund transfers. These entities (collectively called "covered entities") are bound by the privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. If a covered entity engages a BA to help it carry out its health care activities and functions, the covered entity must have a written BA contract or other arrangement with the BA that establishes specifically what the BA has been engaged to do and requires the BA to comply with the HIPAA Rules' requirements to protect the privacy and security of PHI. In addition to these contractual obligations, BAs are directly liable for compliance with certain provisions of the HIPAA Rules.

Question: What is the difference between the Privacy Practices and Procedures requirement and the Notice of Privacy Practices requirement?

Answer: The two requirements serve different purposes and must meet different requirements. Although a covered entity's policies and procedures and its Notice of Privacy Practices somewhat overlap, the policies and procedures should contain a detailed description of all of the entity's privacy practices. In addition, the policies and procedures should provide guidance for the members of the covered entity's workforce who deal with PHI and have responsibility for privacy compliance. On the other hand, the Notice of Privacy Practices is meant to notify participants of the covered entity's practices.

Policy Number: 103

Date of Adoption:

Date of Review/Revision:

HIPAA DOCUMENTATION POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs the creation and maintenance of HIPAA-related documentation for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

Officers, agents, employees, contractors and temporary workers who work for or perform any services (paid or unpaid) for NFP must document all HIPAA-related activities that require documentation and such person's job activities that encompass situations governed by HIPAA. All HIPAA-related documentation must be created and maintained in written form, which may also include electronic forms of documentation.

Any action, activity or assessment that must be documented will be documented in accordance with this and other policies and procedures implemented by NFP. All HIPAA-related documentation must be forwarded, used, applied, filed or stored in accordance with this and other policies and procedures created and implemented by NFP.

Please ensure that all required HIPAA documentation is securely and appropriately maintained and stored in a manner consistent with the HIPAA Privacy and Security Rule Standard and with NFP's policy on document retention outlined in this policy. HIPAA documentation will be made available, as needed, to all workforce members who are authorized to access it and will be made available to appropriate authorities for audits, investigations and other purposes authorized or required by law.

HIPAA documentation will be made available to those workforce members who have a legitimate need for it, and who are authorized to access it, according to current HIPAA Standards. No member of the workforce will be held accountable for compliance with any HIPAA-related documentation, policies, or procedures unless they have been given access to such documentation.

Finally, NFP's policy is to review all HIPAA-related documentation periodically, and update such documentation as needed. Reviews of HIPAA-related documentation will be made periodically, but at least every two years for the purposes of this policy. Reviews and updates of HIPAA-related documentation that occur as a result of this policy will be made by NFP's CPO.

Procedures

Officers, agents, employees, contractors and temporary workers who work for or perform any services (paid or unpaid) for NFP must maintain written or electronic copies of communications that the HIPAA Privacy and Security Rules require to be in writing as also outlined in this policy. Additionally, the workforce members must maintain written or electronic records of actions, activities or designations the HIPAA Privacy and Security Rules require to be documented.

NFP will maintain all documentation as required by the HIPAA Privacy and Security Rules until at least six years after the later of the date of their creation or last effective date.

Please note that this policy pertains to the following HIPAA documentation:

- HIPAA Policies and Procedures.
- HIPAA Risk Analysis.
- Accounting documentation.
- Amendment documentation, including amendment requests.
- All complaints received and their disposition.
- BA contracts and amendments.
- The name and title of the CPO and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
- Training provided.

- Sanctions imposed against non-compliant workforce members.
- Results of analyses that justify release of de-identified information.
- Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.
- All signed authorizations and revocations.
- All approved confidential communication requests and terminations or revocations.

FAQ

Question: With regard to HIPAA, how long must covered entities and BAs retain documentation for the privacy rule?

Answer: NFP will maintain all documentation, as required by the HIPAA Privacy and Security Rules, for 6 years from the date the documentation is created or the date it was last in effect, whichever is later. The documentation under the privacy rule includes any action, activity or designation that the privacy rule requires to be documented. Group health plan brokers are generally considered to be BAs.

Question: Why is the HIPAA Security Rule needed and what is the purpose of the security standards?

Answer: The purpose of the HIPAA Security Rule is to ensure that every covered entity has implemented safeguards to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). Standards for security are needed because there is a growth in the exchange of PHI between covered entities as well as non-covered entities. The standards mandated in the Security Rule protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses and health plans. The Security Rule establishes a Federal floor of standards to ensure the availability, confidentiality and integrity of ePHI. State laws which provide more stringent standards will continue to apply over and above the new Federal security standards.

Question: What constitutes "electronic PHI"?

Answer: "Electronic PHI" or ePHI is defined as PHI that is transmitted by, or maintained in, electronic media. In other words, ePHI is PHI that is stored in computers and the devices that are used with computers, such as disks and drives. EPHI would also include PHI transmitted via email or in any other manner over the internet. However, ePHI does not include PHI on pieces of paper or PHI that is faxed over a dedicated phone line.

Policy Number: 104

Date of Adoption:

Date of Review/Revision:

HIPAA INVESTIGATION POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs HIPAA Investigations for NFP. NFP recognizes that the U.S. Department of Health and Human Services (HHS), it's Office for Civil Rights (OCR), and other designees are all authorized to investigate BAs in matters of HIPAA compliance and enforcement.

NFP managers and supervisors are responsible for enforcing this policy. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS. NFP will not impede or obstruct any HIPAA-related investigations conducted by HHS. Finally, NFP will provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.

Procedures

NFP workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

- Whenever an HHS investigation is discovered, the following persons must be immediately notified:
  - NFP's General Counsel
  - CEO
  - CPO
  - CTO
  - Chief Compliance Officer (CCO)
  - Local HIPAA Privacy Officer
- Cooperate, but do not volunteer information or records that are not requested.
- Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, firm addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call NFP's General Counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. Be sure that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)
- Have at least one, if not two witnesses available to testify to your requests and their responses.
- Determine if there are any law enforcement personnel present (e.g., FBI, US attorneys, state prosecutors). If law enforcement personnel are present, then the investigation is likely a criminal one with much more severe penalties than may result from a civil investigation.
- Permit the investigators to have access to PHI, in accordance with our notice of privacy practices and federal and state law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them if the PHI sought is the subject matter of the investigation or is reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
- Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident. These summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- Do NOT instruct employees to conceal facts or otherwise mislead investigators.
- Ask the investigators for documents related to the investigation. For example, request:
  - Copies of any search warrants and/or entry and inspection orders
  - Copies of any complaints
  - A list of documents/items seized

- Do NOT expect that investigators will provide copies of complaints.
- Do not leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- Do not offer food. (Coffee, if already prepared, and water, if already available, is acceptable). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
- Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the CCO if you are unsure of what or how much to say.
- Maintain written or electronic copies of communications that the HIPAA Privacy and Security Rules require to be in writing as also outlined in this policy.

Additional Information

NFP workforce members who may be interviewed:

- CCO
- CEO
- CPO
- CTO
- Human Resources Representative
- NFP Coordinated Incident Response Team (CIRT)
- Individuals responsible for:
  - Administration of systems which store, transmit or access ePHI
  - Administration systems networks (wired and wireless)
  - Data backup
  - Monitoring of systems which store, transmit, or access ePHI
  - Monitoring systems networks (if different from above)
  - Documents and other information that may be requested for investigations/reviews:

Policies and procedures, and other evidence that address the following:

- Prevention, detection, containment and correction of security violations
- Employee background checks and confidentiality agreements
- Establishing user access for new and existing employees
- List of authentication methods used to identify users authorized to access ePHI
- List of individuals and contractors with access to ePHI
- List of software used to manage and control access to the internet
- Detecting, reporting and responding to security incidents (if not in the security plan)
- Physical security
- Encryption and decryption of ePHI
- Mechanisms to ensure integrity of data during transmission, including portable media transmission (e.g. laptops, cell phones, blackberries, thumb drives)
- Monitoring systems use (authorized and unauthorized)
- Use of wireless networks
- Granting, approving and monitoring systems access
- Sanctions for workforce members in violation of policies and procedures governing ePHI access or use
- Termination of systems access
- Session termination policies and procedures for inactive computer systems
- Policies and procedures for emergency access to electronic information systems

- Password management policies and procedures
- Secure workstation use (documentation of specific guidelines for each class of workstation; i.e., on site, laptop and home system usage)
- Disposal of media and devices containing ePHI

Additional documents:

- Entity-wide security plan
- Risk analysis (most recent)
- Risk management plan (addressing risks identified in the Risk Analysis)
- Security violation monitoring reports
- Vulnerability scanning plans
- Results from most recent vulnerability scan
- Network penetration testing policy and procedure
- Results from most recent network penetration test
- List of all user accounts with access to systems that store, transmit or access ePHI
- Configuration standards to include patch management for systems which store, transmit or access ePHI (including workstations)
- Encryption implemented on systems that store, transmit or access ePHI
- Organization chart to include staff members responsible for general HIPAA compliance to include the protection of ePHI
- Examples of training courses or communications delivered to staff (security awareness training)
- Policies and procedures governing the use of virus protection software
- Data backup procedures
- Disaster recovery plan
- Disaster recovery test plans and results
- Analysis of information systems, applications and data groups according to their criticality and sensitivity
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain ePHI
- List of all Primary Domain Controllers (PDC) and servers
- Inventory log recording the owner and movement media and devices that contain ePHI

FAQ

Question: How does OCR enforce the HIPAA Privacy and Security Rules?

Answer: OCR enforces the Privacy and Security Rules in several ways:

- Investigating complaints filed with it
- Conducting compliance reviews to determine if covered entities are in compliance
- Performing education and outreach to foster compliance with the Rules' requirements

OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

Question: What information would be needed during an OCR investigation?

Answer: That depends on the circumstances and the alleged violations. The HIPAA Privacy Rule limits OCR access to information that is "pertinent to ascertaining compliance." In some cases, no personal health information may be needed. For instance, OCR would need to review only a business contract to determine whether a health plan included appropriate language to protect privacy when it hired an outside company to help process claims.

Policy Number: 105

Date of Adoption:

Date of Review/Revision:

BREACH NOTIFICATION POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs Breach Notifications for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Definitions

As used within the HIPAA Privacy and Security Rules, the following terms have the following meanings:

- Breach means the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy and Security Rules which compromises the security or privacy of the PHI.

  Breach excludes:

  - Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a BA, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA rules.
  - Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or BA to another person authorized to access PHI at the same covered entity or BA, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA rules.
  - A disclosure of PHI where a covered entity or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

  Except as provided above, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA rules is presumed to be a breach unless the covered entity or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated
- Unsecured PHI means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS.

Policy Statement

NFP's policy is to provide timely notifications to the affected covered entity about all breaches of unsecured PHI. Timely notifications to affected covered entities about breaches of IIHI and PHI can help reduce or prevent identity theft and fraud, and can help protect our business and reputation.

NFP will notify the affected covered entity when any breach of unsecured PHI is discovered. A breach is treated as "discovered" by NFP the first day on which such breach is known or should reasonably have been known to any employee or agent of NFP, other than the person who committed the breach.

Finally, NFP understands that the applicable covered entity has an obligation to notify HHS of breaches of unsecured PHI affecting 500 or more individuals and that it may have obligations under its applicable BA Agreement to assist with such notification. Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.

Procedures

Upon discovery of a breach, immediately notify the following individuals:

- NFP's CCO
- NFP's CPO
- Local HIPAA Privacy Officer
- NFP CIRT

Conduct a Breach Risk Assessment and document the following:

- The nature and extent of the PHI involved. Was sensitive data, such as Social Security numbers, claims information or other sensitive information involved in the incident?
- The unauthorized person who used the PHI or to whom the disclosure was made. If the disclosure was made to another HIPAA-regulated entity, there may be a lower probability that the PHI has been compromised because the recipient of the information is obligated to protect the privacy and security of information in a manner similar to NFP.
- Whether the PHI was actually viewed or acquired. This would typically involve a forensic analysis or investigation that could determine whether PHI was contained on a lost or stolen laptop or other portable electronic device was actually viewed or accessed.
- The extent to which the risk to PHI has been mitigated. This might involve reaching out to an unauthorized recipient of the PHI to obtain "satisfactory assurances" that any PHI sent to a recipient was not further used or disclosed but was instead destroyed.

Breach notices must include a brief description of what happened, a description of the types of PHI involved, a brief description of the actions taken in response to the breach, and contact procedures for the covered entity to ask questions and obtain further information.

Telephone and email will be the default methods of notification to the covered entity.

BAs (subcontractors) of NFP are required to immediately report all breaches, losses or compromises of IIHI – whether secured or unsecured – to the CPO. BAs must review their applicable BA Agreement, which will include breach notification requirements. Identify whether NFP has any obligations to notify the affected individuals, HHS, the media or any state regulatory body of a breach.

NFP's CCO will immediately notify NFP's cybersecurity carrier regarding the breach.

Sanctions or re-training will be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to NFP's Sanctions Policy. All breach-related activities and investigations will be thoroughly and timely documented in accordance with NFP's Documentation Policy.

Additional Information

Notification to HHS

The HITECH Act requires covered entities to notify HHS of breaches of unsecured PHI, with the timing of such notification based on the size of the breach. Covered entities must notify HHS of breaches affecting 500 or more individuals and must notify the affected individuals at the same time.

For breaches affecting fewer than 500 individuals, covered entities must notify HHS within 60 days after the end of the calendar year in which the breaches were "discovered," not in which the breaches "occurred."

Notifications to Individuals and Media

Covered entities must notify individuals when a reportable breach is discovered. A breach is treated as "discovered" by the covered entity the first day on which such breach is known or should reasonably have been known to any employee or agent of the covered entity, other than the person who committed the breach.

Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay. Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions. First-class mail is the default method of notification. A covered entity may use email if requested by the individual, or substitute notice via the covered entity's website or local print or broadcast media if the covered entity does not have current contact information.

Covered entities must notify major local media outlets of a breach affecting more than 500 individuals.

BAs must provide notice of breach to a covered entity without unreasonable delay and in no event later than 60 days from discovery of the breach by the BA.

Breaches – Duty to Mitigate Harm Remains

The notification should describe the steps the covered entity or BA is taking to mitigate potential harm to individuals resulting from the breach and that such harm is not limited to economic loss.

FAQ

Question: Who must be notified when there is a breach?

Answer: Upon discovery of a breach, immediately notify the following individuals:

- NFP's CCO
- NFP's CPO
- Local HIPAA Privacy Officer
- NFP CIRT

Question: I emailed some protected information to the wrong client. I've asked the client to delete the information. Do I need to do anything else?

Answer: Yes. Report the incident to NFP's CIRT, which stands ready to respond to any cyber-security incident, even unintended disclosures that are the result of employee mistakes. Alert CIRT of incidents by emailing CIRT@nfp.com or by contacting Mark Grosvenor (mgrosvenor@nfp.com or 512.697.6650) or David Horn (dhorn@nfp.com or 512.697.6508).

Policy Number: 106
Date of Adoption:
Date of Review/Revision:

PRIVACY OFFICER POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs designation of a CPO for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP policy is to designate and maintain at all times an active CPO. NFP, as a BA, recognizes that the designation of a CPO provides numerous benefits to NFP.

The HIPAA Privacy Officer's general responsibilities are to:

- Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
- Conduct various risk analyses as needed or required.
- Manage breach notification investigations, determinations and responses, including breach notifications, in conjunction with the NFP CIRT.
- Develop or obtain appropriate privacy and security training for workforce members.
- Designate as many local HIPAA privacy officers as necessary.

Procedures

NFP's CPO and the officer's local designees will be responsible for implementing, enforcing and maintaining the following procedures:

- Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce and extended workforce, and for all BAs, in cooperation with Human Resources, the CTO, administration and legal counsel (as applicable).
- Maintain an inventory of NFP firms that have access to PHI.
- Cooperate with HHS and its OCR, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
- Develop specific policies and procedures mandated by the HIPAA Privacy and Security Rules.
- Draft and disseminate the Privacy Notice required by the HIPAA Privacy Rule, if applicable.
- Determine when consent or authorization is required for uses or disclosures of PHI and draft forms as necessary.
- Review contracts, when notified of their existence, under which access to confidential data is given to outside entities, and bring those contracts into compliance with the Privacy Rule.
- Work with various personnel to conduct periodic risk assessments and take remedial action as necessary.
- Oversee employee training in the areas of information privacy and security.
- Remain up-to-date on laws, rules and regulations regarding data privacy and update the NFP's HIPAA policies and procedures as necessary.

FAQ

Question: Is the designation of a privacy officer optional for a covered entity or BA?

Answer: No. HHS recognizes that covered entities range from small to large. Therefore, the flexibility and scalability of the HIPAA Privacy and Security Rules are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity or BA will depend on the nature of the covered entity's or BA's business, as well as the covered entity's or BA's size and resources. That said, a covered entity or BA must designate a privacy officer responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's or BA's privacy practices.

Question: What is the difference between the Privacy Practices and Procedures requirement and the Notice of Privacy Practices requirement?

Answer: The two requirements serve different purposes and must meet different requirements. Although a covered entity's policies and procedures and its Notice of Privacy Practices somewhat overlap, the policies and procedures should contain a detailed description of all of the entity's privacy practices. In addition, the policies and procedures should provide guidance for the members of the covered entity's workforce who deal with PHI and are responsible for privacy compliance. On the other hand, the Notice of Privacy Practices is meant to notify participants of the covered entity's practices.

Policy Number: 107
Date of Adoption:
Date of Review/Revision:

HIPAA TRAINING POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs HIPAA Privacy and Security Training for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to provide clear and complete HIPAA training to all members of the workforce, including employees, contractors and temporary workers who have access to PHI as a part of their job responsibilities. HIPAA training provided by NFP will include relevant and appropriate aspects of both health data privacy and health data security, as it pertains to NFP's operations and to the duties and responsibilities of NFP as a BA.

Procedures

HIPAA training, at minimum, will include the basics of HIPAA itself, the basics of HIPAA's privacy and security requirements and restrictions, and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.

HIPAA training will be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with IIHI. Additionally, HIPAA training will be conducted periodically for all employees, but no less than every two years. Documentation of completion will be maintained by Human Resources.

Please note that additional retraining is required in the case of material changes to the privacy policies and procedures of NFP.

The CPO or other designee is responsible for the development or acquisition of appropriate HIPAA training and awareness resources.

FAQ

Question: Generally, what training does the HIPAA Privacy Rule require?

Answer: The Privacy Rule simply requires training employees so that they understand the privacy procedures. The Privacy Rule gives needed flexibility for covered entities to create their own privacy procedures, tailored to fit their size and needs. The training requirement may be satisfied by a small covered entity by providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies, whereas a large covered entity may provide training through live instruction, video presentations or interactive software programs.

Policy Number: 108
Date of Adoption:
Date of Review/Revision:

PHI USES AND DISCLOSURES POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs permitted uses and disclosures of PHI for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to conduct its operations in full compliance with HIPAA's Rules governing uses and disclosures of PHI. For especially sensitive information, such as AIDS/HIV status and substance abuse prevention and treatment histories, patient consent to disclosure must be informed. That is, consent must be made with the patient's or consumer's knowledge of the risks and benefits of the disclosure. Any disclosure of confidential patient information carries with it the potential for an unauthorized re-disclosure that breaches confidentiality.

Definitions

NFP adopts the definitions set forth in the HIPAA regulations at 45 CFR Parts 160, 162 and 164.

- **Authorization:** A document that is required to be signed by the patient to use and disclose specified PHI for specified purposes.
- **Disclosure:** The release, transfer, provision of access to, or divulgence in any other manner, information outside a UAB covered entity maintaining the information.
- **Health Care Operations:** Any of the activities set forth in the regulations that include, but are not limited to the following:
  - Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines; population-based activities relating to improving health or reducing health care costs; protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment
  - Underwriting, premium rating and other activities relating to health plan contracts
  - Conducting medical review, legal services auditing and compliance functions
  - Business planning and development and business management and general administrative activities, including customer service, resolution of internal grievances, and due diligence.
- **Minimum Necessary:** To make reasonable efforts to limit the use or disclosure of, and requests for, PHI to the least amount of PHI necessary to accomplish the intended purpose of the use or disclosure.
- **Payment:** The activities described in the regulation, including determinations of eligibility or coverage; risk adjusting amounts due; billing, claims management, and collection activities; review of health care services with respect to medical necessity and coverage; utilization review activities, including precertification and preauthorization of services; and disclosure to consumer reporting agencies of the following information: name/address, date of birth, social security number, payment history, account number, and name and address of the provider.
- **PHI:** Health information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present or future physical or mental health condition of any 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 that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium. PHI does not include IIHI in employment records held by a covered entity in its role as an employer.

- **Psychotherapy Notes:** Notes recorded by a provider who is a mental health professional documenting or 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. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.
- **Treatment:** The provision, coordination or management of health care services by providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for health care from one provider to another.
- **Use:** The sharing, employment, application, utilization, examination or analysis of PHI within an entity that maintains the PHI.

Procedures

NFP will only use or disclose PHI in accordance with the requirements set forth in this policy and the applicable Business Associate Agreement.

With certain exceptions noted below, when using, disclosing or requesting PHI, NFP will limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The "minimum necessary" standard does not apply to:

- Disclosures to the individual who is the subject of the disclosure
- Uses or disclosures made pursuant to authorization
- Uses or disclosures required by law
- Disclosures to the Secretary of HHS

Whenever an individual's authorization or opportunity to object is required by this policy, NFP will treat personal representatives as the individual for purposes of this standard. "personal representatives" are described as follows:

- Individuals with authority to act on behalf of an adult or emancipated minor in making decisions related to health care
- Executors or administrators acting on behalf of a deceased individual or the individual's estate.

NFP is not required to honor the requests of personal representatives if NFP has a reasonable belief the personal representative is abusing or neglecting the patient or if the entities, in the exercise of professional judgment, decide that it is not in the best interest of the patient to treat the person as the patient's personal representative.

Required Disclosures – NFP must disclose PHI to an individual who requests their own PHI; and to the Secretary of HHS to investigate NFP's compliance with HIPAA.

Permitted Uses and Disclosures – Treatment, Payment or Health care Operations

NFP may use PHI for payment or health care operations except as relates to psychotherapy notes and except as prohibited by the applicable Business Associate Agreement.

Disclosure of PHI:

- For Payment. NFP may disclose PHI to another covered entity for payment activities of that entity.
- For Health Care Operations. NFP may disclose PHI to another covered entity for health care operations in the following situations:
  - The covered entity has a relationship with the individual.
  - The health care operations are quality assessment and improvement activities; case management and care coordination; reviewing the competence or qualification of health care professionals; training programs, accreditation and licensing activities; and compliance activities.
  - If an individual is deceased, NFP may disclose to persons who were involved in payment of care (not just personal representative) prior to the individual's death PHI of the deceased individual that is relevant to that person's involvement unless doing so in inconsistent with any prior expressed preference of the deceased individual made known to the covered entity.
- The following disclosures of PHI do not require subcontractor Business Associate Agreements:
  - To health plans for payment
  - To any entity that is merely serving as a conduit for transmission of the PHI (i.e., telephone companies)
  - Incidental disclosures of PHI (i.e. janitorial staff)

- NFP may use or disclose PHI with no patient consent, authorization, or opportunity to object under any one of the following circumstances:
    - NFP may use or disclose PHI as required by law.
    - Public health activities: NFP may use or disclose PHI to an employer about an employee if the health care is furnished at the request of the employer for medical surveillance of the workplace or a work-related illness or injury and NFP provides written notice to the employee that PHI is disclosed to the employer.
- Reporting of victims of abuse, neglect or domestic violence. NFP may use or disclose PHI to outside entities charged with overseeing victims of abuse, neglect or domestic violence, consistent with reporting obligations under law.
- Health oversight activities. NFP may use or disclose PHI to a health oversight agency for activities authorized by law, i.e., government, licensing, or accreditation agencies.
- Judicial and administrative proceedings.
    - NFP may use or disclose PHI in the course of any judicial or administrative proceeding:
        - In response to an order of a court or administrative tribunal
        - In response to a subpoena, discovery request or other lawful process, if the subpoena or discovery request is accompanied by one of the following:
            - Written documentation from the requesting party that a qualified protective order has been entered or applied for that limits disclosure to the proceedings and requires return or destruction of the PHI at the end of the proceeding
            - Written documentation from the requesting party that the individual has been notified, given an opportunity to object and did not object
- Law enforcement purposes. NFP may use or disclose PHI for law enforcement purposes, as follows:
    - Pursuant to process and as otherwise required by law, i.e., court subpoenas or orders
    - Pursuant to a law enforcement official's request for information to identify and locate a suspect, fugitive, material witness or missing person provided
    - Only the following information is disclosed: name, address, date of birth, Social Security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death (if applicable), and a description of distinguishing physical characteristics
    - The following information will not be disclosed: any PHI related to the individual's DNA or DNA analysis, dental records, or typing samples of analysis of body fluids or tissue
    - Pursuant to a law enforcement official's request for information about an individual who is a victim of a crime, provided that the individual consents to the disclosure
    - If the individual is unable to consent because of incapacity or other emergency circumstances, the information may be released only if the law enforcement official represents that the information is needed for an investigation and will not be used against the victim
    - To alert law enforcement officials about an individual who has died if the death may have resulted from criminal conduct
    - To report evidence of criminal conduct on the premises
- Family members of decedent. NFP may disclose PHI to a family member, other relative, or close personal friend who was involved in the individual's care or payment for care prior to the individual's death, unless the patient previously instructed not to do so.
- Avert a serious threat to health or safety. NFP may use or disclose PHI to prevent a serious threat to the patient's health and safety or the health and safety of the public or another person. The disclosure may only be made to someone able to help prevent the threat.
- Specialized government functions. NFP may use or disclose PHI to military command authorities or federal officials for intelligence and national security activities and protective services, and to correctional institution or law enforcement officials for provision of health care or for the health and safety of others.
- Workers Compensation. NFP may use and disclose PHI to employers and administrators for workers' compensation or similar programs.

- Additional permitted uses and disclosures by covered health plans:
  - NFP, on behalf of a health plan, may disclose to plan sponsor/employer summary health information, if requested by the plan sponsor/employer for the purposes of obtaining premium bids or modifying, amending or terminating the health plan.
  - NFP, on behalf of a health plan, may disclose to the plan sponsor/employer if an individual is participating in, is enrolled in or has disenrolled from a plan.
  - NFP, on behalf of a health plan, may disclose to plan sponsor/employer an individual's medical information for plan administrative functions if the plan sponsor/employer agrees to ensure confidentiality of the information and to not use it for employment-related activities.
  - NFP will not use or disclose PHI that is genetic information for underwriting purposes except as provided by law.

Authorizations

Authorizations are required for all uses and disclosures of PHI not otherwise addressed in this policy. Authorizations must be on an approved HIPAA compliant authorization form. NFP cannot condition the enrollment in a health plan on signing Authorizations for release of PHI, except initial enrollment in health plans can be conditioned on signing an Authorization for the health plan to review PHI to make eligibility determinations.

Individuals may revoke Authorizations by submitting a written revocation to NFP. The revocation will not be effective for any actions taken in reliance on the Authorization prior to receipt of the written revocation. NFP must maintain copies of the Authorizations and any revocations for a period of six years.

FAQ

Question: My state requires consent to use or disclose health information. Does the HIPAA Privacy Rule take away this protection?

Answer: No. The Privacy Rule does not prohibit a covered entity from obtaining an individual's consent to use or disclose his or her health information and, therefore, presents no barrier to the entity's ability to comply with state law requirements.

Question: Is a covered entity required to prevent any incidental use or disclosure of PHI?

Answer: No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures.

Policy Number: 109

Date of Adoption:

Date of Review/Revision:

PATIENTS' RIGHTS POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs the provision and management of Patients' Rights for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Patient information related to patients' rights includes only that information contained in each patient's Designated Record Set (DRS), which is defined in the HIPAA regulations at Section 164.501 as:

- A group of records maintained by or for a covered entity that is:
  - The medical records and billing records about individuals
  - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan
  - Used, in whole or in part, by or for the covered entity to make decisions about individuals.

The term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a covered entity.

Policy Statement

NFP's policy is to provide all the patient rights to our clients' patients and participants that are called for in the HIPAA Privacy and Security Rules.

Patients' rights that NFP provides and supports include:

- The right to review or obtain a copy of medical records about the insured or about the insured's minor children.
- The right to request restrictions on the use or disclosure of the insured's medical records.
- The right to receive IIHI at an alternate address or through alternate delivery means, such as by fax or courier.
- The right to request amendments to medical records, with certain limitations.
- The right to an accounting of certain disclosures of IIHI.
- The right to file a privacy complaint directly with us, or with the federal government.

No retaliation of any kind is permitted against any person, patient or workforce member for exercising any right guaranteed by HIPAA.

Procedures

NFP will only use or disclose PHI in accordance with the requirements set forth in this policy and the applicable BA Agreement.

- **Requesting a Restriction**
  An individual's request for a restriction must be in writing. The request will include the individual's name and contact information; the PHI to which the restriction applies; the requested restriction; the dates on which the restriction is requested to begin and end; the date of the request; and the individual's signature.
- **Processing a Request for Restriction**
  A request for a restriction will be forwarded to the CPO or the Local HIPAA Privacy Officer at the applicable NFP firm. The CPO has the sole authority to grant or deny requests for restrictions. The CPO will respond to all requests for restriction in writing, within 30 days of receiving a request for a restriction.

- The CPO must grant the request if the following criteria are both satisfied:
  - The disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment)
  - The PHI pertains solely to a health care item or service for which the health care provider has been paid in full by the individual

  Except as described immediately above, the CPO will not agree to any restriction that is, in the sole judgment of the CPO, unenforceable. For purposes of this procedure, a restriction is unenforceable if it prevents the use or disclosure of PHI for purposes of carrying out treatment, permitted public interest or benefit activities, or prevents disclosure to the Secretary of HHS for investigation or enforcement.

  The CPO will respond to the individual in writing, advising the individual of the determination.

- **When a Request for Restriction Is Granted**
  - When the plan agrees to a request for restriction, the CPO will notify the affected person in writing of such restrictions. A notation will be made in the individual's record(s). The plan will not use or disclose PHI inconsistent with the restriction.
  - Although a request for restriction has been granted, the plan may disclose the PHI, if requested to do so, for emergency medical treatment of the individual.
- **When a Request for Restriction Is Denied**
  The individual will be given the opportunity to discuss his or her privacy concerns, if desired. Efforts will be made to assist the individual in modifying the request for restrictions to accommodate his or her concerns and obtain acceptance by the plan.
- **Document Retention**
  The CPO will maintain a copy of the determination and any related documents in a file specifically designed for that purpose. The file will be subject to the document retention provisions of these HIPAA Policies and Procedures.
- **Access to PHI**
  An individual has the right to request access to his or her PHI that is in a DRS and is within the plan's control. The plan may deny a request for access only as set forth in these HIPAA Policies and Procedures:
  - An individual's request for access must be in writing. (For purposes of this Policy, "access" may be either inspection of the PHI in question or a copy of such PHI.) The request should include the individual's name and contact information; the PHI to which the request applies (by category or date, as the case may be), the date of the request, and the individual's signature.
  - A request for access will be forwarded to the CPO. The CPO has the sole authority to grant or deny such requests. If the request is granted, access must generally be provided within 30 days (60 days for records maintained offsite), as more specifically provided below. Therefore, the CPO should strive to grant or deny the request within 10 days.

  The plan may deny the individual access to any of the following PHI. Such denial is not subject to review:

  - Psychotherapy notes.
  - Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceedings.
  - PHI maintained by a covered entity that is subject to the Clinical Laboratory Improvement Amendments (CLIA), 42 USC Section 263a, to the extent that access would be prohibited by law.
  - PHI maintained by a covered entity that is exempt from CLIA pursuant to 42 CFR Section 493.3(a)(2).
  - PHI contained in records that are subject to the Privacy Act, 5 USC Section 552a, if the denial meets the requirements of that law.
  - PHI obtained from someone other than a health care provider under a promise of confidentiality, provided that the access would be reasonably likely to reveal the source of the information.

  The plan may deny the individual access to PHI in any of the following circumstances. Such denial is subject to review:

  - A licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to endanger the life or physical safety of the individual or another person.
  - The PHI makes reference to another person (other than a health care provider), and a licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to cause substantial harm to such other person.
  - The request for access is made by the individual's personal representative, and a licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to cause substantial harm to the individual or another person.

  When the plan denies access to only part of the PHI, the plan will provide access to the remainder of the PHI.

When a Request for Access is **denied**:

- The plan will provide the individual with a statement, written in plain language, that includes:
  - The reasons for the denial.
  - If applicable, a statement that the individual has a right to a review of the denial by a licensed health professional who is designated by the plan but who did not participate in the original decision to deny access.
  - If applicable, the individual's right to a review of the decision with an explanation of how to exercise this right.
  - A description of how the individual may file a complaint with the plan and the Secretary of HHS, including the title and telephone number of the plan's contact person.
  - If the denial is prepared by someone other than the CPO, a copy of the denial will be forwarded to the CPO.
  - To the extent possible, the plan will grant access to other PHI for which there are no grounds to deny access.

When a Request for Access is **granted**:

- If the request for access is granted, the CPO will notify the individual of the decision in writing. Access to on-site records will be provided within 30 days after receipt of the request, and access to off-site records will be provided no later than 60 days after receipt of the request.
- The plan will offer access to the individual in the form of inspection, or copying, or both, as the individual may choose.
- The plan will produce the PHI in the form or format requested by the individual, including electronic format, if the PHI is readable and producible in that format.
- The plan may charge a fee for copying or other reproduction, as described below.
  - The plan will charge a reasonable, cost-based fee for copying, including labor and supplies (for instance, paper, computer disks, flash drives).
  - The plan will charge the cost of postage when the individual requests that the information be mailed.
  - No fee is charged for retrieving or handling the PHI or for processing the individual's access request.
  - The plan may charge a nominal fee for preparing an explanation or summary of the requested PHI if the individual is informed of and agrees to receive a summary of the PHI and is willing to pay the fee.
  - The CPO will determine the appropriate amount of the fee, and will inform the individual in advance so that the individual has the opportunity to elect to withdraw or modify the request to reduce or avoid the fee.

- **Accounting**

  Individuals have a right to an accounting of the plan's disclosures of their PHI. As set forth in these HIPAA Policies and Procedures, Certain disclosures are not required to be included in the accounting. All disclosures of PHI are accountable except the following:

  - Disclosures to carry out treatment, payment or health care operations (however, disclosures to carry out treatment, payment or health care operations are accountable if they are made through an electronic health record)
  - Disclosures made to (or for notification of) persons who are involved in an individual's health care or who are involved in payment related to that health care
  - Disclosures made more than 6 years before the date of the request for accounting (3 years in the case of a disclosure made through an electronic health record)
  - Disclosures to the individual, or the individual's personal representative, about his own PHI
  - Disclosures incident to a use or disclosure permitted or required by the Rule
  - Disclosures made for disaster relief
  - Disclosures pursuant to an authorization
  - Disclosures for national security or intelligence purposes
  - Disclosures to correctional institutions or a law enforcement officer regarding inmates or persons in lawful custody

  Processing a Request for Accounting:

- All requests for accounting will be forwarded to the CPO. Only the CPO may respond to a request for accounting on behalf of the plan.
- Upon receipt of a request for an accounting, the CPO will:
  - Determine if there are fees for the individual's accounting and notify the individual of such fees in advance of compiling the accounting.
  - If the request includes disclosures made by one or more BA of the plan, the CPO may request the necessary information from the affected BA and include the information provided by the BA in the plan's accounting or respond to the request with an accounting of disclosures made by the plan and provide the individual with contact information for the BA.
  - Gather the necessary information.
  - Respond in writing to the individual's request within 60 days. If the plan is unable to make its determination within such 60-day period, the plan may obtain an extension for no more than 30 days. The plan can obtain this extension only by providing written notice of the extension to the individual within the original 60-day period. The written notice will explain the reason for the delay and the date by which the plan will provide the accounting. If the notice is prepared by someone other than the CPO, a copy of the notice will be forwarded to the CPO.
  - Forward the request for the accounting and the accounting itself to the CPO, who will maintain a copy in a file specifically designed for that purpose. The file will be subject to the document retention provisions of these Privacy Policies and Procedures.

Content of Accounting:

- For each accountable disclosure of PHI the accounting provided to the individual will include all of the following:
  - The disclosure date.
  - The name and address (if known) of each person or entity that received the disclosure.
  - A description of the PHI disclosed.
  - A statement of the purpose of the disclosure, or, if the PHI was disclosed pursuant to a public interest or benefit activity, a copy of any written request for the disclosure from the Secretary of HHS or another government agency.

FAQ

Question: Does an individual have a right under the HIPAA Privacy Rule to restrict PHI his or her health care provider discloses for workers' compensation purposes?

Answer: Individuals do not have a right under the Privacy Rule to request that a covered entity restrict a disclosure of PHI about them for workers' compensation purposes when that disclosure is required by law or authorized by, and necessary to comply with, a workers' compensation or similar law.

Policy Number: 110
Date of Adoption:
Date of Review/Revision:

PRIVACY COMPLAINTS POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs the privacy complaints process for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to respond in a timely and positive manner to all complaints submitted by any persons or parties, including insureds, workforce members, and any other person or party. Responsibility for the acceptance of, management of and responses to complaints will reside with the designated CPO who will establish a process and appropriate forms to receive and process complaints.

Procedures

All complaints must be submitted in written form, dated and signed by the complainant.

NFP will investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant will be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the complaint. In no case will more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.

The CPO or other responsible party will investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, will be interviewed in a non-threatening and non-coercive manner.

The final resolution or disposition of each complaint will be documented in accordance with the NFP HIPAA Documentation Policy, and will be retained in accordance with NFP's Record Documentation Retention Policy. A summary of the findings will be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30 days of response time is invoked, as above.

In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediation may include, but is not limited to:

- A written apology to the complainant from our organization.
- Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured IIHI that has been compromised or put at risk by our actions.
- Financial compensation, if determined to be appropriate by legal counsel and NFP senior management.
- Sanctions against workforce members, as appropriate to the circumstances.
- Other unspecified remediation(s), as determined by legal counsel and NFP senior management.

For complaints submitted to the federal government, it is the Policy of NFP to cooperate fully and openly with federal authorities as they conduct their investigation, as specified. No officer, agent, employee, contractor, temporary worker or volunteer of NFP will obstruct or impede any investigation in any way, whether internal or federal.

FAQ

Question: If I believe that my privacy rights have been violated, when can I submit a complaint?

Answer: The OCR provides the following information on how to file a complaint.

- Activities occurring before April 14, 2003, are not subject to OCR enforcement actions.
- After that date, a person who believes a covered entity is not complying with a requirement of the HIPAA Privacy Rule may file with OCR a written complaint, either on paper or electronically.
- This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred.
- OCR may waive this 180-day time limit for good cause.

In addition, individuals have a right to file a complaint directly with the covered entity under their privacy practices.

Policy Number: 111

Date of Adoption:

Date of Review/Revision:

RISK MANAGEMENT POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs the establishment and maintenance of a risk management process for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

The scope of risk analysis that the HIPAA Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that an organization creates, receives, maintains or transmits.

Policy Statement

NFP's policy is to establish, implement and maintain an appropriate risk management process. Such a risk management process will be under the direct control and supervision of the CPO and CTO and will involve legal counsel, information technology, NFP senior management, and any other parties or persons deemed to be appropriate to the process.

Business and information-technology "best practices," along with the research and recommendations of the National Institute for Standards and Technology (NIST), will be included in the development and execution of the risk management process. Overall, NFP's risk management process will strive to identify, analyze, prioritize and minimize identified risks to information privacy, security, integrity and availability. The nature and severity of various risk and risk elements will be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process will be ongoing, and will be updated, analyzed and improved on a continuous basis.

Procedures

NFP will conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI that NFP is entrusted with. The results of the risk management process will be used for management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

A risk assessment is required when a new project is started, regardless of whether the solution is custom, installing of a third party or a combination of multiple solutions. This assessment will be performed within the scope of the project and will only consider factors and equipment outside the project when it affects the risk to the project.

A risk assessment should also be performed when any application/infrastructure is modified enough to add, remove or modify data such that the sensitivity and security requirements may change or data associated with the organization is sent/stored in a different location than when the last security assessment was performed. This assessment will consider the change in risk due to the modifications to the existing infrastructure, systems and/or processes.

The risk analysis process will be modeled upon the risk analysis process recommended by the NIST. All such risk analyses and assessments will be documented in accordance with the NFP HIPAA Documentation Policy and HIPAA's Privacy and Security Rules.

FAQ

Question: Is the use of encryption mandatory in the HIPAA Security Rule?

Answer: The final Security Rule made the use of encryption an addressable implementation specification. Therefore, the encryption implementation specification must be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of ePHI. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate. If the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure and document the rationale for this decision.

Question: Is a covered entity legally required to conduct a HIPAA compliance audit of its BAs?

Answer: HIPAA doesn't impose a specific requirement that a covered entity audit its BAs. That said, ERISA requires fiduciaries of a group health plan to select the plan's service providers prudently and to monitor the performance of the service providers. Thus, there is some fiduciary responsibility to monitor a BA's activity, and a HIPAA compliance audit could be one way of meeting that responsibility. In that light, a covered entity may want to reserve the right to audit their BAs in the BA Agreement. That way, if a covered entity suspects that a BA has violated the BA Agreement, the covered entity, as part of its investigation of the problem, may want to undertake a HIPAA compliance audit to determine whether the BA has in fact violated the agreement.

Policy Number: 112
Date of Adoption:
Date of Review/Revision:

SANCTIONS POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs workforce sanctions and disciplinary actions for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to establish and implement appropriate, fair and consistent sanctions for workforce members who fail to follow established HIPAA policies and procedures, or who commit various offenses. Appropriate, fair and consistent sanctions have a deterrent influence on workforce transgressions, can help prevent breaches of IIHI and PHI, and can help prevent (or reduce the severity) of HIPAA violations.

Sanctions applied will be appropriate to the nature and severity of the error or offense, and will consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses and more severe sanctions applied to more severe errors and offenses. Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.

NFP's policy is to fully document all workforce sanctions and their dispositions, according to our NFP HIPAA Documentation Policy and HIPAA requirements.

Procedures

Upon report of a workforce member's violation of NFP's privacy policies and procedures, the CPO will contact the CCO and Human Resources to determine appropriate sanctions in accordance with the policies outlined above.

FAQ

Question: Is a covered entity liable for, or required to monitor, the actions of its BAs?

Answer: The HIPAA Privacy Rule requires covered entities to enter into written agreements or other arrangements with BAs that protect the privacy of PHI, but covered entities are not required to monitor or oversee the means by which their BAs carry out privacy safeguards or the extent to which the BA abides by the privacy requirements of the agreement. Moreover, the covered entity is not responsible or liable for the actions of its BAs. However, if a covered entity finds out about a material breach or violation of the agreement by the BA, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the agreement with the BA. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to HHS.

With respect to BAs, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of PHI to the BA are not permitted. In cases where a covered entity is also a BA, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a BA of another covered entity.

Policy Number: 113
Date of Adoption:
Date of Review/Revision:

ASSIGNMENT OF SECURITY RESPONSIBILITY POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs the assignment of responsibility for health information data security for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP policy is to assign responsibility for the overall security of IIHI, in electronic and other forms, to a person or person(s) who are qualified to assume such responsibility. The assignment of overall security and responsibility is an important and integral part of our overall risk management process, and will be conducted in accordance and coordination with NFP's risk management and securities policies. The persons with overall responsibility for the security of IIHI, in electronic and other forms, will be the CCO, CTO and CPO.

Procedures

The CCO, CTO and CPO or other responsible party who has been designated by the CCO, CTO or CPO will implement the following procedures, as appropriate:

- Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in NFP's workforce, extended workforce and for all BAs in cooperation with Human Resources as applicable.
- Administer the process for receiving, documenting, tracking and investigating, and taking action on complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Cooperate with the HHS, OCR, other legal entities, and others in the organization in any compliance reviews or investigations.
- Develop policies and procedures mandated by the HIPAA Privacy and Security Rules.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Address questions concerning when an NFP organization needs consent or authorization for use of disclosure of PHI, and draft forms as necessary.
- Oversee employee training in the area of privacy.
- Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain up-to-date and advise on new technologies to protect data privacy.
- Remain up-to-date on laws, rules and regulations regarding data privacy and update NFP's policies and procedures as necessary.
- Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
- Serve as a liaison to government agencies, industry groups and privacy activists in all matters relating to NFP's privacy practices.

Policy Number: 114
Date of Adoption:
Date of Review/Revision:

WORKFORCE CLEARANCE POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs workforce clearance and screening (pre-employment and post-employment) for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP policy is to provide the appropriate level of access to IIHI to all members of its workforce. Providing appropriate workforce clearance can help reduce the likelihood of data breaches and HIPAA violations. The level of access to IIHI for workforce members will be based upon the nature of each workforce member's job and its associated duties and responsibilities. Workforce members will have access to all of the IIHI that they need to do their jobs, but no more access than that.

Procedures

Workforce clearance will specifically incorporate various levels of background screening to ensure that persons with criminal records or histories of financial or legal difficulties do not have inappropriate access to IIHI. The CCO, or other designated person, will coordinate background screening requirements with Human Resources and the CPO to ensure that appropriate background screening requirements are established and met. The CCO, or other designated person, will also coordinate proper supervision of workforce members processing PHI as a part of their job function.

FAQ

Question: What does the HIPAA Security Rule mean by physical safeguards?

Answer: Physical safeguards are physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity's premises or at another location.

Policy Number: 115

Date of Adoption:

Date of Review/Revision:

ACCESS TERMINATION POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs termination of individual access to IIHI and PHI for NFP. All NFP workforce members must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to terminate any workforce member's access to IIHI and PHI when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy. Prompt and appropriate termination of workforce member access to IIHI and PHI can greatly reduce the likelihood of data breaches and HIPAA violations.

Termination of workforce member's access to IIHI and PHI must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy violation or HIPAA offense.

NFP's policy is to fully document all access termination-related activities, in accordance with the NFP HIPAA Documentation Policy.

Procedures

NFP has a termination process in place that ensures employees, contractors and third-party users exit the organization or change employment in an orderly manner. Specifically, this process includes procedures to ensure that all equipment is returned and that the removal of all access rights is completed. NFP's process is as follows:

- Termination requests will be sent to or created by Human Resources.
- Terminations will be processed following a standard process and using the ticketing system.
- Access regulated by the domain controller will be terminated as soon as Technology Services is notified, which will eliminate access to NFP systems.
- Tickets for removing access to individual applications will be processed in a timely fashion.

Policy Number: 116

Date of Adoption:

Date of Review/Revision:

ACCESS AUTHORIZATION POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs the authorization and granting of access to IIHI and PHI to workforce members for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to grant workforce members an appropriate level of access to IIHI and PHI that is based on their work-related duties and responsibilities. The implementation of appropriate processes to grant workforce members access to IIHI and PHI can help ensure that our uses and disclosures of IIHI are lawful and appropriate. The level of access to IIHI and PHI granted to each member of the workforce will be independent of the technology used to access such information, and will apply to access through a workstation, transaction, program, process or other mechanism. NFP's policy is to fully document all access authorization-related activities and efforts.

Procedures

User Access Administration

Access Control is the process of assuring that only properly approved users are granted access to information. The goals of user Access Administration are to permit access to information and technology resources on a need-to-know basis according to job function and to ensure that users are prevented from gaining access to information and technology for which they are not authorized.

The user Access Administration policy guidance is set forth below:

- Business unit managers must authorize access to information and technology.
- Access to information and technology must be on a need-to-know, job function basis. Users must only have the minimum access rights and privileges needed to perform a particular function or transaction.
- At least annually, a review of user access rights to information and technology must be conducted.
- At least semi-annually, a review of user IDs not used within the last six months should be conducted by the business unit to determine if these user IDs should be disabled or deleted.
- Access to technical system documentation (e.g., application documentation and user manuals) should be restricted on a need-to-know, job-function basis.
- A business unit manager should notify the security administrator immediately upon transfer, change of job responsibilities or leave of absence of a user.
- When a security administrator is notified that a user has transferred, changed job responsibilities or taken a leave of absence, the security administrator should immediately take steps to ensure that the user's access privileges are revoked if those privileges no longer apply.
- User accounts that have attempted to log in unsuccessfully five times should be locked until a system administrator unlocks them or until 30 minutes have passed.
- If there are 10 or more unsuccessful login attempts within a 24 hour period, the account will be permanently locked until unlocked by a system administrator.

Monitoring

Monitoring is the process of gathering information related to the interaction between users and information. This information provides a means of reconstructing events for investigative purposes and establishing individual accountability. The goals of monitoring are to provide for the logging of events and provide a mechanism to retrieve and report information on logged events.

Specific security events should be recorded, including:

- Successful session log-ins.
- Identification and authentication failures.
- Security administration activity.
- All activities performed by privileged users.
- Failed attempts to access information.

Specific information should be included in the tracking record associated with each event:

- User identifier.
- Information or system accessed.
- Date and time of access.
- Type of event.
- Result of event.
- Reason for failure (if applicable).

In addition, monitoring should include:

- The identity of the user, or processes acting on behalf of the user, should be maintained for the duration of the session. For example, change of operational mode or privileges should not result in the loss of uniqueness of a user.
- Accountability tracking information should be maintained for a minimum of three months after it is collected. Retention may be extended by legal, regulatory or investigative requirements.
- To allow proper remedial action, the operational area, the business unit or information security personnel should review records reflecting security relevant events in a periodic and timely manner.

Policy Number: 117
Date of Adoption:
Date of Review/Revision:

ACCESS ESTABLISHMENT AND MODIFICATION POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs establishment and modification of access to IIHI and PHI for workforce members for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to provide a lawful and appropriate level of access to IIHI for all relevant workforce members. Establishing, maintaining and modifying appropriate levels of workforce member access to IIHI and PHI can help reduce the likelihood of data breaches and HIPAA violations. The level of access to IIHI and PHI will be granted based on the nature and duties of the workforce member's job duties. Workforce members' access to IIHI will be modified immediately when the nature of the job changes and requires a different level of access, whether greater or lesser. NFP's policy is to fully document all access authorization-related activities and efforts.

Procedures

Web Identity, Access Management, and Dual Factor Authentication

NFP employs least-privilege access for specific duties and systems making use of an industry-leading role-based identity and access management suite of products along with dual-factor authentication for secure authorization, authentication and accounting. Password strength and expiration rules are managed centrally and adhere to NFP's Enterprise IT policy and industry best practices.

Identification and Authentication

- Each user must be uniquely identified. For example, a system user ID must not be assigned to more than one person, and each user must have an individually identifiable ID.
- Each user must be identified and authenticated before performing any actions on the system.
- The authentication process is limited to five unsuccessful attempts. When this limit is reached, the user identifier should be disabled.
- Identification and authentication should both be completely processed by the system prior to displaying the failed attempt indicator. All messages associated with failed log-ins should be non-descriptive.
- Only a Security Administrator or equivalent will have the access entitlements necessary to reset a disabled user ID.
- A user identifier that has been inactive for a period of 90 days should be disabled. The intervention of a security administrator should be required to reset the disabled user ID. If an exception to this is required, the business unit manager should approve the exception condition in writing.
- A message should appear on all internal computing systems prior to any logos or banners, and before the initial Identification and Authentication process.

User Access Administration

Access administration is the process of assuring that only properly approved users are granted access to information. The goals of user access administration are to permit access to information and technology resources on a need-to-know basis according to job function and to ensure that users are prevented from gaining access to information and technology for which they are not authorized.

The user access administration policy guidance is set forth below:

- Business unit managers must authorize access to information and technology.

- Access to information and technology must be on a need-to-know, job-function basis. Users must only have the minimum access rights and privileges needed to perform a particular function or transaction.
- At least annually, a review of user access rights to information and technology must be conducted.
- At least semi-annually, a review of user IDs not used within the last six months should be conducted by the business unit to determine if these user IDs should be disabled or deleted.
- Access to technical system documentation (e.g., application documentation and user manuals) should be restricted on a need-to-know, job-function basis.
- A business unit manager should notify the security administrator immediately upon transfer, change of job responsibilities or leave of absence of a user.
- When a security administrator is notified that a user has transferred, changed job responsibilities or taken a leave of absence, the security administrator should immediately take steps to ensure that the user's access privileges are revoked if those privileges no longer apply.
- User accounts that have attempted to log in five times unsuccessfully should be locked until a system administrator unlocks them or until 30 minutes have passed.
- If there are 10 or more unsuccessful login attempts within a 24 hour period, the account will be permanently locked until unlocked by a system administrator.

Monitoring

Monitoring is the process of gathering information related to the interaction between users and information. This information provides a means of reconstructing events for investigative purposes and establishing individual accountability. The goals of monitoring are to provide for the logging of events and provide a mechanism to retrieve and report information on logged events.

Specific security events should be recorded, including:

- Successful session log-ins
- Identification and authentication failures
- Security administration activity
- All activities performed by privileged users
- Failed attempts to access information

Specific information should be included in the tracking record associated with each event:

- User identifier
- Information or system accessed
- Date and time of access
- Type of event
- Result of event
- Reason for failure (if applicable)

In addition, monitoring should include:

- The identity of the user, or processes acting on behalf of the user, should be maintained for the duration of the session. For example, change of operational mode or privileges should not result in the loss of uniqueness of a user.
- Accountability tracking information should be maintained for a minimum of three months after it is collected. Retention may be extended by legal, regulatory or investigative requirements.
- To allow proper remedial action, the operational area, business unit or information security personnel should review records reflecting security relevant events in a periodic and timely manner.

Policy Number: 118

Date of Adoption:

Date of Review/Revision:

SECURITY AWARENESS AND TRAINING

Scope of Policy

This policy governs the creation and implementation of a security awareness and training program for all members of NFP's workforce (including management). All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations.

It is the Policy of NFP to:

- Develop and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
- Establish a program of regular monitoring and review of log-ins and log-in attempts.
- Fully document all access authorization-related activities and efforts.
- Fully document all log-in monitoring-related activities and efforts.
- Develop and apply a rigorous program of techniques, technologies and methods to guard against, detect and report the presence of malicious software.
- Fully document all malware protection-related activities and efforts, in accordance with the NFP HIPAA Documentation Policy.
- Require the use of strong passwords and pass-phrases by all workforce members who access, use or maintain systems that contain, transmit, receive or use IIHI.

The CPO, CTO, or other designated responsible party will assume responsibility for developing or acquiring such resources for implementing a plan and program to ensure their frequent use. The CPO, CTO, or other designated responsible party will also be responsible for ensuring that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the IIHI they contain.

Discrepancies and potentially inappropriate or illegal activities will immediately be brought to the attention of NFP senior management as appropriate.

Procedures

Passwords or Pass-Phrases

- All passwords or pass-phrases used to access systems containing, transmitting, receiving, or using IIHI will be a minimum of six characters in length, and must include non-alphanumeric characters or symbols in them, unless protected by multi-factor authentications (MFA). Passwords for applications protected with MFA should be at least twelve characters and need not contain non-alphanumeric characters or symbols.
- Passwords and pass-phrases should be changed by users at least every six months, unless application is protected by MFA.
- In the event of an information system compromise, as determined by the CTO, some or all workforce-member passwords and pass-phrases may need to be changed. This determination will be made by the CTO.
- Under no circumstances will passwords or pass-phrases be written down and kept at or near computers and workstations where they may be found by others.
- Any workforce member who loses, misplaces, forgets or experiences any compromise of their password or pass-phrase will immediately notify the Technology Department.

- Proper password management will be emphasized in HIPAA training programs, in security reminders, and in any HIPAA awareness resources used by NFP.

Training

- Overall, training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure and how to report discrepancies, and user education in password management.
- Upon hire, all members of NFP's workforce must take cyber-security training and HIPAA training.
- All members of NFP's workforce must renew their cyber-security training annually and their HIPAA training every other year.
- Human Resources will monitor to assure that required training courses are completed and that all members of NFP's workforce are up to date with training requirements. Individuals and, when necessary, managers will be notified of any lapses to ensure that all are in compliance with this policy.
- NFP also has required monthly supplemental training on IT security topics, which is also monitored for compliance.
- If any member of NFP's workforce falls for a phishing scam (real or test), that person will receive an email with detailed information about phishing scams and how to detect them. If there is a second incident, that person will be required to take a one-hour remedial course on IT security.

FAQ

Question: In limiting access, are covered entities required to completely restructure existing workflow systems, including upgrading computer systems, in order to comply with the HIPAA Privacy Rule's minimum necessary requirements?

Answer: The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to protected health information to those in the workforce that need access based on their roles in the covered entity.

Generally, HHS does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Policy Number: 119
Date of Adoption:
Date of Review/Revision:

POLICY FOR BUSINESS ASSOCIATES ON SECURITY INCIDENT PROCEDURES

Scope of Policy

This policy governs responses to Security Incidents involving the breach or compromise of PHI for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

In today's fast-paced and interconnected business environment, even with careful adherence to industry best practices and regulations, organizations can expect that cybersecurity breaches, criminal activity or disaster incidents will occur. When these events happen, limiting their impact while protecting the assets, operations and reputation of the organization requires a coordinated and timely response.

To this end, NFP has chartered the NFP Coordinated Incident Response Team (CIRT) and prepared the Cyber-Security Incident Response Plan (CSIRP) maintained by the CIRT to prepare the organization's response posture for when such incidents occur. NFP's policy is to rapidly identify and appropriately respond to all security incidents, regardless of their severity. The responsibility for responding to and managing security incidents will reside with the NFP CIRT.

Procedures

In addition to the procedures outlined below, please see the CSIRP maintained by the CIRT. The objective of the CSIRP is to define and disseminate the methods and procedures to be used in response to any disruption or suspected/verified cyber-security/criminal incidents, with the goal of returning NFP to a "trusted state" for continuing business operations.

The CIRT is a cross-functional team consisting of representatives from several NFP Departments, including:

- Legal/Compliance.
- Public Relations/Marketing.
- Human Resources.
- Risk Management.
- Information Technology.

The CIRT is charged with ensuring that incidents reported to it are handled in a manner that:

- Prioritizes human safety.
- Contains or eliminates the threat to the information assets in a timely manner.
- Provides accurate communications to stakeholders.
- Complies with applicable laws and regulations.
- Allows for ongoing detective or forensics review as needed.
- Fully remediates the problem.
- Provides protection against additional potential loss/inconvenience to clients and employees.
- Ensures the public's trust in NFP as a service provider and custodian of information assets.
- Restores normal business operations.
- Are reported to NFP's Board and Compliance and Ethics Committees during standing updates.

The CIRT may also proactively inform and recommend operational improvements to NFP Executive Management that reduce risk, educate staff and generally improve NFP readiness against future incidents.

The CIRT will be chaired by the CTO. The CIRT will report findings directly to the Executive Management Committee and other interested stakeholders, regulatory bodies or law enforcement as NFP deems appropriate.

All incidents reported to the CIRT will be logged for future review or reference.

The CIRT is NOT directly responsible for:

- Management of information technology or security infrastructure or staff
- Detection of potential cybersecurity events
- Audit or compliance reviews of NFP firms or departments

The CIRT can be assembled by emailing the team at CIRT@nfp.com or contacting Mark Grosvenor, CTO, at mgrosvenor@nfp.com or P: 512.697.6650.

FAQ

Question: I emailed some protected information to the wrong client. I've asked the client to delete the information. Do I need to do anything else?

Answer: Yes. Report the incident to NFP's CIRT, which stands ready to respond to any cybersecurity incident, even unintended disclosures that are the result of employee mistakes. Alert CIRT of incidents by emailing CIRT@nfp.com or by contacting Mark Grosvenor (mgrosvenor@nfp.com or 512.697.6650) or David Horn (dhorn@nfp.com or 512.697.6508).

Policy Number: 120
Date of Adoption:
Date of Review/Revision:

DATA BACKUP AND STORAGE POLICY FOR BUSINESS ASSOCIATES

Scope of Policy

This policy governs data backup and Storage for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

The ability to create and maintain retrievable, exact copies of ePHI is a critical element of our business operations and our ability to respond to unexpected negative events. The storage of data backups in a separate location, removed from our normal business operations (off-site) is an essential element of any successful data backup plan.

NFP policy is to create and maintain complete, retrievable, exact backups of all ePHI stored in the course of business operations in full compliance with all the requirements of HIPAA. All data backups will be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times. The CTO is responsible for performing appropriate backups on NFP's network, including shared drives containing application data, patient information, financial data and crucial system information.

Procedures

Information Technology recognizes that the backup and maintenance of data for servers and storage are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

Backups are performed with the following schedule:

- **Real Time –** Backups are performed in real time to the Austin data center and the cloud.
- **Daily Differential Backups –** Daily differential backups are performed Monday through Friday and are stored in the NY datacenter then replicated to the Austin datacenter.
- **Full Backups –** Full backups are performed once a week for each server and are stored in the NY datacenter then replicated to the Austin datacenter. Each weekend, full tape jobs are run with the tapes going off-site Monday to a third-party vendor for storage and to be kept indefinitely.

FAQ

Question: May a HIPAA covered entity or business associate use a cloud service to store or process ePHI?

Answer: Yes, provided the covered entity or business associate enters into a HIPAA-compliant business associate contract or agreement with the cloud service provider that will be creating, receiving, maintaining or transmitting ePHI on its behalf, and otherwise complies with the HIPAA Rules.

Policy Number: 121

Date of Adoption:

Date of Review/Revision:

DISASTER RECOVERY POLICY

Scope of Policy

This policy governs contingency Disaster Recovery Planning for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

HIPAA requires NFP to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, natural disaster, etc.) that damage systems containing ePHI. It is the Policy of NFP to create and maintain complete, retrievable copies of ePHI in full compliance with all the requirements of HIPAA. A disaster may occur at any time, not necessarily during work hours. NFP must remain operational with as little disruption of business operations as possible.

Procedures

In addition to the procedures outlined below, please see the NFP Business Continuity Plan (BCP) maintained by the BCP Coordination Committee.

Business Impact

Today with our fast-paced and interconnected business environments there can be many events that might cause the interruption of services. These "disasters" can include natural disasters, accidents, power or communication interruptions, sabotage/terrorism/cyberattacks, technology systems failures, and medical emergencies. Creating and maintaining the NFP BCP should help NFP procure the resources and information needed to deal with disasters in the event that they occur.

Each type of disaster comes with its own unique characteristics and challenges. Each incident comes with many different risks that vary with the actual situation. Some events would cause only minor disruptions and be resolved in a relatively short period of time, with minimum financial impact. Other events or combinations of events might cause longer-term disruptions with catastrophic financial consequences.

Risk can be assessed in accordance to potential severity (example: high, medium, low) and the probability of occurring (example: likely and unlikely – high, medium, low likelihood). The BCP has tried to assess these risks and their potential impact on the company and how best to incorporate them.

Business Continuity Plan Guidelines

NFP has developed plans that include the ability to recover from and to continue operations that might result for various natural and man-made disaster situations. These occurrences could result from situations that include but are not limited to, unplanned evacuations, power outages, severe weather, building facilities problems, computer/software and other technological problems, communication problems, medical emergencies, and other such unexpected events.

On a continuous basis NFP tries to mitigate its risk to reduce the impact of unplanned disasters which might affect its business operations however not all occurrences can be planned and protected from. Some of the key guidelines and functions are:

- Employee safety: NFP places emphasis on the safety of its employees by training its employees on safety and evacuation procedures.
- Employee BCP training: Key employees are kept current and trained on what action steps might be necessary in the event of business interruption disaster.
- Backup power and data: NFP has on-site generators at corporate locations that output electrical power to operate its critical corporate-provided IT systems and back up data on a regular basis.

- Separate sites: In the event of a major disaster, NFP has firms across the country that will act as backup facilities for NFP locations that are impacted by a disaster. NFP also maintains a contract with an external offsite facility to support operations of the larger corporate offices and their operations should the corporate buildings become uninhabitable or cut off.
- Many NFP systems are redundantly hosted by the chosen cloud provider so that in the event of a disaster the accessibility, reliability and accuracy of the key business systems are not impacted and can be accessible from alternate, non-impacted areas.
- NFP works with key third-party providers to be sure that their systems, operations and personnel also have sufficient BCP's and operations/technical redundancy established and can be invoked in the event of a disaster.

These are just a few of the many steps that NFP is prepared to take in the event of a business disaster that impacts operations at any one of its firms. This plan is a tool designed to enable NFP and the firms to continue business operations in the event that a significant business interruption should occur.

Policy Number: 122

Date of Adoption:

Date of Review/Revision:

EMERGENCY MODE OPERATIONS POLICY

Scope of Policy

This policy governs Emergency Mode Operations and planning for NFP. NFP will establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to establish this Emergency Mode Operations Policy to implement procedures to enable continuation of critical business processes for the protection of IIHI while operating in emergency mode. IIHI must be protected during emergencies, even as it is protected during normal operations. This Emergency Mode Operations Policy is designed to ensure the protection and availability of PHI during emergencies requiring NFP to operate in "emergency mode."

Our Emergency Mode Operations Plan must be implemented and executed in coordination with other emergency and/or disaster plans and procedures, as appropriate and necessary. NFP's policy is to fully document all emergency planning and preparedness activities and efforts, in accordance with our Documentation Policy.

Procedures

Our Emergency Mode Operations Plan will be executed whenever NFP must operate in emergency mode.

Implementation of the Plan

This Plan has been designed to be implemented in the event of a disaster that results in a significant business disruption to NFP or an NFP Firm. Whether all or only parts of the Plan are implemented depends on the nature of the disruption. Generally, a significant business disruption would include:

- Destruction of one of the firm's facilities, whether by natural causes or by other means;
- Loss of life or major injuries to personnel in a firm location that disables that firm's ability to conduct business and support customer needs
- Disruption of service from a critical service provider

This NFP Firm has designated an Emergency Response Team that is responsible for implementing necessary procedures included in this Plan. The Response Team's action will depend on the nature and scope of the disruption. The "first responder" has the primary responsibility for taking action, and the "secondary responder" acts as a back-up in the event the first responder is unable to act. Where feasible, the two responders are located in different firm locations.

Action	First Responder/Location	Secondary Responder/Location
Contact emergency services such as police, fire department		
Establish off-site command center and notify employees		
Contact employees regarding Plan initiatives		
For affected firms evaluate business disruption and transfer employees and business operations to other locations		
Appoint individuals to manage business areas where needed		
Assess financial and operations capabilities		
Determine financial and credit risk and contact banks and other counter-parties, if necessary, to secure financing to continue operations		
Notify regulators in the event of a capital deficiency		

Action	First Responder/Location	Secondary Responder/Location
Interface with SIPC if liquidation of business is initiated		
Contact critical service providers		
Transfer mission critical functions that are disrupted to Alternative Location(s)		
Initiate alternative customer communications systems or procedures		
Notify customers regarding alternative access to insurance, 401K, funds and securities		
Recover back-up records when primary records are destroyed or inaccessible		
Contact regulators and notify them of contact persons and recovery plans		

Emergency Contact List

This NFP firm has established an Emergency Contact List that includes the names, phone numbers (cell and land lines), email addresses and other contact information for individuals critical to the firm's business including key employees, key vendors or service providers, regulators, insurance carriers, banks, attorneys, and other key contacts. A copy of the list is provided to each member of the Response Team and other key personnel. This list will be reviewed and updated on at least an annual basis.

Computers and peripherals

Hardware will be leveraged from the New York/Austin Corporate offices, nearby NFP firms or bought at local stores.

Alternative Business Locations

In the event employees can no longer conduct business at one of the NFP firm's locations, the following actions may be taken:

- Transfer employees to the closest unaffected location and notify personnel.
- Transfer critical systems to another NFP firm or a back-up firm or system.
- Transfer business operations to another NFP firm unaffected by the disruption.
- Transfer business operations to a different broker-dealer or other entity.
- Transfer business operations to the New York office.

Data Backup and Recovery

This NFP firm maintains its books and records in both hard copy and electronic format.

In the event of an internal or external significant business disruption that causes the loss of the firm's records (whether hard copy or electronic records), backup records will be recovered from the backup site.

Clearing Firms Backup and Recovery

For NFPSI, the clearing firm maintains records for the firm under the terms of the clearing agreements. The clearing firm has developed a disaster and recovery plan to recover and retrieve records lost in a disaster affecting the firm and/or the clearing firm. Records retained by the clearing firm are included on the firm's Books and Records chart.

This NFP firm has received assurance from the clearing firm that its plan is consistent with SRO rule requirements and provides adequate protection of customer funds and securities held on behalf of firm customers and backup and recovery systems for records retained by the clearing firm. Compliance (or another person designated to review critical third party plans) will review the clearing firms plan or a summary of the plan at least annually when the firm's Plan is reviewed.

Mission Critical Systems

Mission critical systems are systems that are necessary to ensure prompt and accurate processing of insurance, 401K, benefits, securities transactions including order taking, entry, execution, comparison, allocation, clearance and settlement, maintaining customer accounts, and providing access to customer funds and securities.

This document identifies systems (or generally describes procedures) that are critical to the operation of the firm's business; identifies third parties that provide those systems; and potential alternate procedures or systems for handling these critical functions in the case of a disruption.

Recovery Time Objective and Recovery Point Objective

NFP has set the following for Recovery Time Objectives (RTO) and Recovery Point Objective (RPO):

- RTO for business critical systems including e-mail and data storage – 8 hours
- RTO for all other systems including remote access through the VPN – 24 hours
- RPO – 30 minutes

Policy Number: 123

Date of Adoption:

Date of Review/Revision:

POLICY ON TESTING AND REVISION OF CONTINGENCY AND EMERGENCY PLANS

Scope of Policy

This policy governs Testing and Revision of Contingency and Emergency Plans for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce that has access to PHI as a part of their job function.

Policy Statement

NFP's policy is to periodically test all emergency preparedness plans and revise them as necessary, including emergency and contingency plans. Emergency contingency plans and the procedures associated with them must be periodically tested and revised to ensure that they meet the emergency preparedness needs of NFP.

NFP's policy is to ensure that all IIHI, including PHI, will be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Procedures

Emergency and contingency plans are the responsibility of the CPO, CTO or other designated responsible party, who will ensure that all such plans are up-to-date and meet our emergency preparedness requirements.

Emergency contingency plans will be reviewed at least annually and revised if necessary. Copies of all such plans will remain on file and be available to all personnel. Emergency and contingency plans will be rehearsed at least annually, with all team members participating.

Some material events that require revision of the plans, include:

- Material changes to the NFP firm's business.
- A change in the NFP firm's main office location.
- Added firm locations.
- A change in a major service provider.

When the plan is reviewed, the procedures and accompanying lists and charts will be reviewed and updated as needed including the:

- Plan itself.
- Emergency Response Team list.
- Emergency Contact List.

The CPO, CTO or other designated responsible party, will fully document all emergency preparedness plans, including emergency and contingency plans, and all the revisions thereto, in accordance with the NFP HIPAA Documentation Policy and the requirements of HIPAA.

Policy Number: 124

Date of Adoption:

Date of Review/Revision:

POLICY ON DATA AND APPLICATIONS CRITICALITY ANALYSES

Scope of Policy

This policy governs Data and Applications Criticality Analyses for NFP. Assess the relative criticality of specific applications and data in support of other contingency plan components. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP policy is to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations. A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting IHII, including PHI, during emergencies and during normal business operations

Procedures

Data to be subject to criticality analysis will include IHII, including PHI. Criticality analysis will be the responsibility of the CPO, CTO or other designated responsible party, who will work in cooperation as necessary to execute and document such analyses.

Criticality analyses will determine and document the relative criticality of each type or category of data and applications that NFP possesses and/or uses to the continuity and success of our operations. The most critical data and applications will be given the highest priority in terms of investment and emergency protection preparations, with less critical categories or types of data and applications receiving proportionately less funding and attention as appropriate.

NFP reviews and defines the various types of data that are housed in NFP systems and/or accessible by NFP employees and contractors. The three types of classifications defined in this policy are: Confidential, Sensitive and Public. The NFP Database Administration Team is ultimately responsible for deciding how to classify data.

Data classifications will be reviewed periodically to confirm that they are still appropriate based on changes to legal, regulatory and contractual obligations as well as changes in the use of the data. The Database Administration Lead must determine the frequency that is most appropriate based on need. If the Database Administration Lead determines that the classification of a certain data set has changed, an analysis of security controls must be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they must be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

Data collection

NFP will limit the amount and type of the information gathered to what is necessary for the identified purposes. NFP employees and contractors will be trained to explain to customers why the information is needed.

Data Types

NFP has defined three data types and created a data classification for each: Confidential, Sensitive and Public. The following sections will define these data and provide examples of each type.

Confidential

Data is classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to NFP's clients, business, carriers or affiliates. Users of Confidential data must follow all safeguards for Sensitive data plus additional safeguards identified for confidential data.

IIHI

IIHI that consists of an individual's name, including the last name along with the individual's first name or first initial, in combination with and linked to any one or more of the following data elements:

- Social Security number or partial Social Security number
- Driver's license number
- State identification card number
- Passport number
- United States Permanent Resident Card or similar identification
- SSID – Statewide Student Identifier
- Financial account number
- Credit card number
- Debit card number
- Electronically stored biometric information

PHI

- Patient names
- Street address, city, county, zip code
- Dates (except year) related to an individual, e.g., clinical encounters
- Email, URLs, & IP addresses
- Social Security numbers or partial Social Security numbers
- Account/medical record numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifications and serial numbers
- Device identifications and serial numbers
- Biometric identifiers
- Full face images associated with HIPAA records
- Payment guarantor's information

Legal Information

- All data in the Office of the General Counsel unless otherwise classified by the General Counsel.

Sensitive

Data is classified as Sensitive when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to NFP or its affiliates. By default, all data that is not explicitly classified as Confidential or Public data must be treated as Sensitive data. A reasonable level of security safeguards must be applied to Sensitive data.

The following table contains examples of Sensitive data.

- Client Name
- Date of birth
- Place of birth
- Physical address
- Mailing address
- Phone number
- Email address
- Secondary mailing or permanent address

Public

Data that is readily available to the public. This data requires no confidentiality or integrity protection.

If a data type is not defined or classified, it should be assumed to be Confidential until it has been classified. Any potential leakages of data against this policy should be immediately reported to the NFP CIRT so that proper steps for remediation can be followed.

In conducting data and applications analyses, the CPO, CTO or other designated responsible party will employ the technical guidance and recommendations of the NIST, and/or other information technology best practices as appropriate. The CPO, CTO or other designated responsible party will fully document all analyses of the relative criticality of both data and applications, in accordance with the NFP HIPAA Documentation Policy and the requirements of HIPAA.

Policy Number: 125

Date of Adoption:

Date of Review/Revision:

POLICY ON EVALUATING THE EFFECTIVENESS OF SECURITY POLICIES

Scope of Policy

This policy governs periodic Evaluations of the Effectiveness of Security Policies for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to periodically evaluate security policies, including emergency and contingency plans and procedures, in order to improve their effectiveness. Security policies, including emergency and contingency plans and procedures, must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

Procedures

It will be the responsibility of the CPO, CTO or other designated responsible party to periodically conduct such technical and nontechnical evaluations. The CPO, CTO or other designated responsible party will work in coordination with legal counsel, information technology, NFP senior management, and any other persons, departments or parties necessary in order to conduct such evaluations. Such technical and nontechnical evaluations will be conducted at least annually.

The results of such technical and nontechnical evaluations will be internally published and will be available to NFP senior management and to all parties with responsibility for emergency preparedness.

The purpose of such evaluations is to improve the effectiveness of our security policies, including emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the IIHI, including PHI that NFP possesses or uses.

Some material events that require revision of the plans, include:

- Material changes to the NFP firm's business.
- A change in the NFP firm's main office location.
- Added firm locations.
- A change in a major service provider.

When the plan is reviewed, the procedures and accompanying lists and charts will be reviewed and updated as needed including the:

- Plan itself.
- Emergency Response Team list.
- Emergency Contact List.

The CPO, CTO or other designated responsible party will fully document our periodic technical and nontechnical evaluations to determine the effectiveness of our security policies, including emergency and contingency plans and procedures, in accordance with the NFP HIPAA Documentation Policy and the requirements of HIPAA.

Policy Number: 126
Date of Adoption:
Date of Review/Revision:

BUSINESS ASSOCIATES POLICY

Scope of Policy

This policy governs relationships with and operations involving BAs of NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to establish and maintain lawful working relationships with our own BAs that are in full compliance with all the requirements of the HIPAA Final "Omnibus" Rule. NFP recognizes its status as a BA under the definitions contained in the HIPAA rules.

In cooperation with our organization, subcontractors who our BAs work with, use, transmit, and/or receive IIHI, including PHI, which is afforded specific protections under HIPAA. NFP has the primary responsibility in all BA relationships to ensure that IIHI, including PHI, is properly protected and safeguarded.

The HIPAA Privacy and Security Rules specifically identify the following types of entities as BAs:

- Subcontractors.
- Patient safety organizations.
- HIOs: Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
- E-Prescribing gateways.
- PHRs: Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of CEs are not BAs.
- Other firms or persons who "facilitate data transmission" that requires routine access to PHI.

The "Minimum Necessary Standard" now applies directly to BAs. HIPAA now applies the Minimum Necessary standard directly to BAs and their subcontractors. When using, disclosing or requesting PHI, all these entities must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Subcontractors of BAs are now BAs themselves. A subcontractor is defined as a person or entity to whom a BA delegates a function, activity or service involving PHI, and who is not a member of the BA's own workforce. As a BA itself, NFP is required to enter into a BA contract with any subcontractor who is a BA of ours.

Procedures

Responsibility for maintaining appropriate and lawful relationships with BAs will reside with the CPO, CTO or other designated responsible party who will ensure that all aspects of our BA relationships are appropriate and lawful, and who will ensure that IIHI, including PHI, is properly protected and safeguarded by our BAs.

With regard to our own BAs (subcontractors), the duties and responsibilities of the CPO, CTO or other designated responsible party will include, but are not limited to the following:

- Ensure that all BA agreements meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, the HIPAA "Omnibus" Final Rule, and any requirements of state laws in the state(s) where NFP operates.
- Ensure that IIHI, including PHI, is properly protected and safeguarded by our BAs.
- Ensure that BAs understand the importance and necessity of protecting IIHI, including PHI, whether in ePHI or hardcopy form.
- Ensure that BAs have proper and appropriate safeguards in place for IIHI, including PHI, before entrusting such information to them.

- Ensure that BAs understand and are properly prepared to detect and respond to breaches of IIHI, including PHI.

The CPO, CTO or other designated responsible party will fully document all BA-related agreements and activities, in accordance with our Documentation Policy and the requirements of HIPAA.

FAQ

Question: What are some examples of an entity that is a BA?

Answer: The HIPAA Privacy and Security Rules specifically identify the following types of entities as BAs:

- Subcontractors.
- Patient safety organizations.
- HIOs: Health Information Organizations (and similar organizations).
- E-Prescribing gateways.
- PHRs: Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of CEs are not BAs.
- Other firms or persons who "facilitate data transmission" that requires routine access to PHI.

Question: What is the purpose of having a business associate agreement?

Answer: The business associate agreement (BAA) establishes the permitted and required uses and disclosures of PHI by the business associate performing activities or services for the covered entity or business associate, based on the relationship between the parties and the activities or services being performed by the business associate. The BAA also contractually requires the business associate to appropriately safeguard the PHI, including implementing the requirements of the HIPAA Privacy and Security Rule.

Policy Number: 127
Date of Adoption:
Date of Review/Revision:

FACILITY ACCESS CONTROL POLICY

Scope of Policy

This policy governs the Facility Security and maintenance records, as well as the Access Control and Validation Procedures for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to:

- Provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for IIHI, including PHI.
- Create and maintain complete facility security maintenance records, including repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks), in full compliance with all the requirements of HIPAA.
- Implement and support strong and ongoing access control and validation procedures in full compliance with all the requirements of HIPAA.
- Fully document all facility security-related activities and efforts, and access control and validation procedures in accordance with our Documentation Policy.

In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for IIHI, including PHI. Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security, as detailed in our Facility Security Plan.

Access control and validation procedures are designed to control and validate individual access to facilities based on role or function, including visitor control and access control for software testing and revision. Strong access control and validation procedures are an essential element of protecting IIHI, including PHI.

Responsibility for planning and executing facility security, access control and validation procedures, and maintenance records for NFP operations will reside with the CPO, CTO or other designated responsible party. The CPO, CTO or other designated responsible party will prepare, analyze, test and update plans for such operations on a periodic basis to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.

Procedures

The analyses of our facility security should include, but are not limited to, the following factors:

- Windows and doors.
- Roofs and the potential for roof access.
- Locks and keys.
- Electronic access control systems.
- Video cameras and video surveillance systems.
- Electronic alarms and related systems.
- Employee, partner, vendor and guest access.
- Vehicle parking security.
- Routine and non-routine deliveries.

The development and implementation of specific access control and validation procedures will be conducted in accordance with guidance and information provided by the NIST, or other information technology best practices. NFP employs policies and physical controls focused on allowing the minimum required access to facilities for all parties including employees, contractors and visitors.

Visitor Access

Visitor access to NFP-integrated facilities will be granted with care and carefully monitored. All visitors should meet the following requirements:

- All visitors should enter at the reception area.

- Unknown visitors must show a government identification.
- Visitors must demonstrate a legitimate reason to be visiting the facility, such as a job interview, vendor demonstration or other relevant business activity.
- Visitors must be approved by an authority in the position to grant access.
- Visitors must sign in, record arrival time, what organization they are from (if applicable), and who they are meeting or reason for visiting.
- The NFP employee being met with must escort the visitor in and monitor the visitor's time at the facility. Visitors must be escorted by an NFP employee at all times.
- Access to guest Wi-Fi should be granted for non-NFP business purposes.
- Access to corporate Wi-Fi, NFP computers, or NFP networks is strictly granted to employees and contractors of NFP and will not be shared with visitors.

NFP Employees' Responsibility for Physical Access

- NFP employees should not allow "piggybacking" of anyone they do not know into badge-restricted areas. Employees should endeavor to ascertain the identity of anyone entering or attempting to enter these area and escalate if that identity cannot be determined.

Access to areas with sensitive hardware

Areas containing sensitive hardware should follow industry best practices, including:

- Visitor and vendor access to areas with sensitive hardware should be planned, logged and explicitly approved by corporate IT.
- Any unplanned visitors and/or vendors requesting access to sensitive hardware should be escalated to Technology Services before access is granted.
- Sensitive hardware should be segregated from general use office space.
- Access to sensitive areas (e.g., data centers, telecommunications closets) should be limited to authorized personnel with a legitimate business need.
- A quarterly review will be conducted of individuals with access to sensitive areas.
- Sensitive areas should be monitored by video, and include a motion-detector alarm, as well as a system for detecting glass breakage (if applicable).

Visitor Log Retention

Visitor logs will be retained for a minimum of two years.

FAQ

Question: What does the HIPAA Security Rule mean by physical safeguards?

Answer: Physical safeguards are physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity's premises or at another location.

Policy Number: 128

Date of Adoption:

Date of Review/Revision:

WORKSTATION USE AND SECURITY POLICY

Scope of Policy

This policy governs Workstation Use and Security for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to configure, operate and maintain our information workstations in full compliance with all the requirements of HIPAA. The establishment and implementation of an effective workstation use and security policy is a crucial element in our overall objective of providing reasonable protections for IIHI, including PHI.

Our objective in these efforts is to providing reasonable protections for IIHI, including PHI. Specific procedures will be developed to specify the proper functions, procedures and appropriate environments of workstations that access IIHI, including PHI.

Responsibility for the development and implementation of this workstation security policy, and any procedures associated with it, will reside with the CPO, CTO or other designated responsible party, who will ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization. Specific procedures will be developed to implement physical safeguards for all workstations that access IIHI, including PHI, to restrict access to authorized users only.

NFP's policy is to fully document all workstation use-related activities and efforts, in accordance with the NFP HIPAA Documentation Policy.

Procedures

Mobile Device & Laptop Data and Physical Security

The protection of NFP's mobile assets and the data they may contain is paramount. The following outlines NFP's Mobile Device & Laptop Data and Physical Security Policy:

While in the office:

- All laptops that have the ability must be fitted with a cable lock secured to the user's desk.
- When leaving a laptop unattended for any extended period of time, the user must physically secure the laptop with a cable lock or store it away in a locked cabinet or locked office.
- Users must always log off before leaving their workspace.
- All laptops must have full disk encryption software installed and a method of validation.
- All laptops must have a password protected screen saver that starts automatically after ten minutes of inactivity.

While out of the office:

- Laptops, tablets and smartphones (mobile devices) cannot be left in a vehicle for any extended period of time or overnight.
- In "vulnerable" situations (e.g., public areas such as airport lounges, hotels and conference centers) the mobile devices must never be left unattended; where possible the user should lock mobile devices in a hotel safe or otherwise secure the mobile devices with a cable lock.
- When boarding a plane, mobile devices should not be checked into baggage and should always be part of the user's carry-on items.
- Only secure internet connections should be used to conduct sensitive or confidential business. Examples of unsecured connections include, but are not limited to:
  - Public computers or digital copiers in hotels, airport office centers or other centers (e.g., public cafés).
  - Open, unsecured wireless internet lines available through hotspots.

When knowingly carrying sensitive information:

- Sensitive information must be stored on a secured and backed-up company file storage location.
- Sensitive information or files should not be transferred to media such as USB memory keys, CDs, DVDs, floppy disks or other portable data storage devices.
- Documents with sensitive or confidential information must be password-protected. Emailing these documents must be restricted to NFP's secure and encrypted email platform.

FAQ

Question: What does the HIPAA Security Rule mean by physical safeguards?

Answer: Physical safeguards are physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity's premises or at another location.

Policy Number: 129

Date of Adoption:

Date of Review/Revision:

MEDIA DISPOSAL AND REUSE POLICY

Scope of Policy

This policy governs the Accountability of Information Systems Hardware and Media, Media Disposal and the Reuse of Information Storage Media for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to dispose of all media containing IIHI, including PHI, in full compliance with all the requirements of HIPAA. Moreover, NFP's policy is to properly erase and or sanitize ("wipe") all media containing IIHI, including PHI, before any media may be reused. Responsibility for proper media disposal and disposition will reside with the CPO, CTO or other designated responsible party, who will develop procedures to ensure the proper disposition of all such media.

NFP's policy is to fully document all media reuse and disposal-related activities and efforts, in accordance with our Documentation Policy. NFP also maintains records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.

Overall, media containing IIHI, including PHI, must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.

Procedures

Asset Tracking Requirements

The following procedures and protocols apply to Asset Management Activities:

- Assets will be tracked by their unique identifier (typically serial number, MAC address or service tag number).
- NFP will employ an asset tracking database to record and track assets. This database will generally include the following data (where applicable):
  - Date of purchase.
  - Make, model, and description of device or hardware.
  - Serial number, MAC address, service tag or other unique identifier.
  - NFP location where deployed.
  - Type of asset.
  - PO number (where applicable).
  - Disposition (i.e., status).
- Equipment entering and exiting datacenters requires a ticket.

Asset Disposal

The following procedure/protocol defines how asset management will be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport or disposal.

When disposing of any asset, all sensitive and NFP-related data must be removed. NFP will employ appropriate data destruction protocols to ensure erasure. At a minimum, data must be removed using low level-formatting and the overwriting of media with reasonably secure wiping techniques. NFP will retain certification of any media destruction, where applicable.

FAQ

Question: What are some examples of proper disposal methods?

Answer: Generally, examples of proper disposal methods may include, but are not limited to:

- For PHI in paper records: shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable and otherwise cannot be reconstructed.
- For PHI on electronic media: clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating or shredding).

Policy Number: 130

Date of Adoption:

Date of Review/Revision:

ACCESS CONTROL POLICY

Scope of Policy

This policy governs the issuance, maintenance and security of access to NFP's information systems. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to exclusively use unique user identifications for all information system access and activities, in full compliance with all the requirements of HIPAA. Additionally, NFP's policy is to establish and implement encryption and decryption procedures, in full compliance with all the requirements of HIPAA. Finally, NFP's policy is to always use automatic log off applications or systems on all workstations and computers, in full compliance with the requirements of HIPAA.

Specific procedures will be developed to specify the proper functions and procedures of our automatic log off systems on all computers and workstations that access IIHI, including PHI. Additionally, specific procedures will be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access IIHI, including PHI. The establishment and implementation of an effective automatic log off and encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for IIHI, including PHI.

Responsibility for the development and implementation of this policy regarding the use of unique user IDs, automatic log off applications, and encryption and decryption, will reside with the CPO, CTO or other designated responsible party, who will ensure that access to all our information systems and data is accomplished exclusively through the use of unique user IDs, and who will ensure that these policies are maintained, updated as necessary, and implemented fully throughout our organization.

Nothing in this policy will limit the use of additional security measures, including login and access measures that can further enhance the security and protection NFP provides to IIHI, including PHI.

NFP's policy is to fully document all activities and efforts, in accordance with the NFP HIPAA Documentation Policy.

Procedures

Identification and Authentication

Identification is the process of uniquely distinguishing one user from another to establish accountability. Authentication is the process of verifying the identity of a user. The goals of Identification and Authentication are to establish the identity of a user, verify the claimed identity, and provide accountability for the actions that the user performs.

The Identification and Authentication policy guidance is set forth below:

- Each user must be uniquely identified. For example, a system user ID must not be assigned to more than one person, and each user must have an individually identifiable ID.
- Each user must be identified and authenticated before performing any actions on the system.
- The authentication process is limited to five unsuccessful attempts. When this limit is reached, the user identifier should be disabled.
- Identification and authentication should both be completely processed by the system prior to displaying the failed attempt indicator. All messages associated with failed logins should be non-descriptive.
- Only a Security Administrator or equivalent will have the access entitlements necessary to reset a disabled user ID.
- A user identifier that has been inactive for a period of 90 days should be disabled. The intervention of a Security Administrator should be required to reset the disabled user ID. If an exception to this is required, the business unit manager should approve the exception condition in writing.

User Access Administration

Access control is the process of assuring that only properly approved users are granted access to information. The goals of user access administration are to permit access to information and technology resources on a need-to-know basis according to job function and to ensure that users are prevented from gaining access to information and technology for which they are not authorized.

The user Access Administration policy guidance is set forth below:

- Business unit managers must authorize access to information and technology.
- Access to information and technology must be on a need-to-know, job-function basis. Users must only have the minimum access rights and privileges needed to perform a particular function or transaction.
- At least annually, a review of user access rights to information and technology must be conducted.
- At least semi-annually, a review of user IDs not used within the last six months should be conducted by the business unit to determine if these user IDs should be disabled or deleted.
- Access to technical system documentation (e.g., application documentation and user manuals) should be restricted on a need-to-know, job-function basis.
- A business unit manager should notify the security administrator immediately upon transfer, change of job responsibilities or leave of absence of a user.
- When a security administrator is notified that a user has transferred, changed job responsibilities or taken a leave of absence, the security administrator should immediately take steps to ensure that the user's access privileges are revoked if those privileges no longer apply.
- User accounts that have attempted to log in five times unsuccessfully should be locked until a system administrator unlocks them or until 30 minutes have passed.
- If there are 10 or more unsuccessful login attempts within a 24 hour period, the account will be permanently locked until unlocked by a system administrator.

Monitoring

Monitoring is the process of gathering information related to the interaction between users and information. This information provides a means of reconstructing events for investigative purposes and establishing individual accountability. The goals of monitoring are to provide for the logging of events and provide a mechanism to retrieve and report information on logged events.

Specific security events should be recorded, including:

- Successful session logins.
- Identification and authentication failures.
- Security administration activity.
- All activities performed by privileged users.
- Failed attempts to access information.

Specific information should be included in the tracking record associated with each event:

- User identifier.
- Information or system accessed.
- Date and time of access.
- Type of event.
- Result of event.
- Reason for failure (if applicable).

In addition, monitoring should include:

- The identity of the user, or processes acting on behalf of the user, should be maintained for the duration of the session. For example, change of operational mode or privileges should not result in the loss of uniqueness of a user.
- Accountability tracking information should be maintained for a minimum of three months after it is collected. Retention may be extended by legal, regulatory or investigative requirements.
- To allow proper remedial action, the operational area, business unit or information security personnel should review records reflecting security relevant events in a periodic and timely manner.

Mobile Device & Laptop Data and Physical Security

All laptops must have a password protected screen saver that starts automatically after ten minutes of inactivity. All mobile phones must have a password protected screen saver that starts automatically after ten minutes of inactivity.

Device Encryption

All end-user devices, servers and application data stores are encrypted.

Email Security and Encryption

NFP encrypts emails in transit when identified (manually or through automated algorithms) as containing PHI, PII or other sensitive information. NFP uses third-party mechanisms to protect incoming and outgoing message queues from receiving or sending malicious content, including the vetting of all payloads and links contained therein.

Web Identity, Access Management, and Dual Factor Authentication

NFP employs least-privilege access for specific duties and systems making use of an industry-leading role-based identity and access management suite of products along with dual-factor authentication for secure authorization, authentication, and accounting. Password strength and expiration rules are managed centrally and adhere to NFP's Enterprise IT policy and industry best practices.

Database Security & Classification

System administration and database security is managed by internal NFP staff. SQL accounts are bound by the same password policy as the Active Directory domain. Access to individual client data in a database is restricted by application role-based security. Sensitive client data in the database is encrypted.

Unstructured Data Storage and Transit

All file and data repositories are strictly secured by logical access control policies. Sensitive unstructured data is encrypted in flight through HTTPS, FTPS or SFTP.

FAQ

Question: A member of our workforce attempted to log in numerous times unsuccessfully. Their account is now locked. What should they do?

Answer: User accounts that have attempted to log in five times unsuccessfully should be locked until a system administrator unlocks them or until 30 minutes have passed. If there are 10 or more unsuccessful login attempts within a 24 hour period, the account will be permanently locked until unlocked by a system administrator.

Question: What is the difference between identification and authentication?

Answer: Identification is the process of uniquely distinguishing one user from another to establish accountability. Authentication is the process of verifying the identity of a user. The goals of identification and authentication are to establish the identity of a user, verify the claimed identity, and provide accountability for the actions that the user performs.

Policy Number: 131
Date of Adoption:
Date of Review/Revision:

AUDIT CONTROLS POLICY

Scope of Policy

This policy governs Audit Controls for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

The establishment and implementation of an effective audit controls policy, including hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI, is a crucial element in our overall objective or providing reasonable protections for IIHI, including PHI.

Specific procedures will be developed to specify the proper usage and application of audit controls for all computers, workstations and systems that access IIHI, including PHI. Responsibility for the development and implementation of this audit controls policy and any procedures associated with it will reside with the CPO, CTO or other designated responsible party, who will ensure that this policy is maintained, updated as necessary and implemented fully throughout our organization.

NFP's policy is to fully document all audit control-related activities and efforts, in accordance with the NFP HIPAA Documentation Policy.

Procedures

Monitoring

Monitoring is the process of gathering information related to the interaction between users and information. This information provides a means of reconstructing events for investigative purposes and establishing individual accountability. The goals of Monitoring are to provide for the logging of events and provide a mechanism to retrieve and report information on logged events.

Specific security events should be recorded, including:

- Successful session logins.
- Identification and authentication failures.
- Security administration activity.
- All activities performed by privileged users.
- Failed attempts to access information.

Specific information should be included in the tracking record associated with each event:

- User identifier.
- Information or system accessed.
- Date and time of access.
- Type of event.
- Result of event.
- Reason for failure (if applicable).In addition, monitoring should include:
- The identity of the user, or processes acting on behalf of the user, should be maintained for the duration of the session. For example, change of operational mode or privileges should not result in the loss of uniqueness of a user.
- Accountability tracking information should be maintained for a minimum of three months after it is collected. Retention may be extended by legal, regulatory or investigative requirements.
- To allow proper remedial action, the operational area, business unit or information security personnel should review records reflecting security relevant events in a periodic and timely manner.

FAQ

Question: Does the HIPAA Security Rule mandate minimum operating system requirements for the personal computer systems used by a covered entity?

Answer: No. The Security Rule was written to allow flexibility for covered entities to implement security measures that best fit their organizational needs. The Security Rule does not specify minimum requirements for personal computer operating systems, but it does mandate requirements for information systems that contain EPHI. Therefore, as part of the information system, the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security.

Policy Number: 132

Date of Adoption:

Date of Review/Revision:

DATA INTEGRITY CONTROLS POLICY

Scope of Policy

This policy governs Data Integrity Controls for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA. The purpose of this policy is to ensure that EPHI has not been altered or destroyed in an unauthorized manner. The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for IIHI, including PHI.

Specific procedures will be developed to specify the proper usage and application of data integrity controls for all computers, workstations and systems that access IIHI, including PHI. Responsibility for the development and implementation of this data integrity controls policy and any procedures associated with it will reside with the CPO, CTO or other designated responsible party, who will ensure that this policy is maintained, updated as necessary and implemented fully throughout our organization.

NFP's policy is to fully document all data integrity controls-related activities and efforts, in accordance with the NFP HIPAA Documentation Policy.

Procedures

Device Encryption

All end-user devices, servers and application data stores are encrypted.

Email Security and Encryption

NFP encrypts emails in transit when identified (manually or through automated algorithms) as containing PHI, PII or other sensitive information. NFP uses third-party mechanisms to protect incoming and outgoing message queues from receiving or sending malicious content, including the vetting of all payloads and links contained therein.

Web Identity, Access Management, and Dual Factor Authentication

NFP employs least-privilege access for specific duties and systems making use of an industry-leading role-based identity and access management suite of products along with dual-factor authentication for secure authorization, authentication and accounting. Password strength and expiration rules are managed centrally and adhere to NFP's Enterprise IT policy and industry best practices.

Database Security & Classification

System administration and database security is managed by internal NFP staff. SQL accounts are bound by the same password policy as the Active Directory domain. Access to individual client data in a database is restricted by application role-based security. Sensitive client data in the database is encrypted.

Unstructured Data Storage and Transit

All file and data repositories are strictly secured by logical access control policies. Sensitive unstructured data is encrypted in flight through HTTPS, FTPS or SFTP.

Development Operations Security

NFP software development practices adhere to industry best practices. NFP's internal software development controls are subject to both internal and third-party audit. Segregation of duties between Development, Quality Assurance and Production zones ensures proper source code integrity and controls.

Anti-Virus and Persistent Threat Scanning

NFP leverages multiple, real-time, industry-leading, third-party solutions to continuously scan end points for virus, malware and malicious code signatures.

FAQ

Question: What constitutes ePHI?

Answer: Electronic PHI or ePHI is defined as PHI that is transmitted by, or maintained in, electronic media. In other words, ePHI is PHI that is stored in computers and the devices that are used with computers, such as disks and drives. EPHI would also include PHI transmitted via email or in any other manner over the internet. However, ePHI does not include PHI on pieces of paper or PHI that is faxed over a dedicated phone line.

Policy Number: 133

Date of Adoption:

Date of Review/Revision:

PERSON OR ENTITY AUTHENTICATION POLICY

Scope of Policy

This policy governs Authentication of Persons or Entities seeking access to ePHI in the possession of NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA. The purpose of this Person or Entity Authentication Policy is to ensure that ePHI can only be accessed by persons or entities who are in fact who they claim to be, and not imposters. The establishment and implementation of an effective Person or Entity Authentication Policy is a crucial element in our overall objective or providing reasonable protections for IIHI, including PHI.

Specific procedures will be developed to specify the proper authentication of persons and entities who request access to IIHI, including PHI on our computers, workstations and systems. Responsibility for the development and implementation of this policy and any procedures associated with it will reside with the CPO, CTO or other designated responsible party, who will ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.

NFP's policy is to fully document all person or entity-related activities and efforts, in accordance with the NFP HIPAA Documentation Policy.

Procedures

Identification and Authentication

Identification is the process of uniquely distinguishing one user from another to establish accountability. Authentication is the process of verifying the identity of a user. The goals of Identification and Authentication are to establish the identity of a user, verify the claimed identity, and provide accountability for the actions that the user performs.

The Identification and Authentication policy guidance is set forth below:

- Each user must be uniquely identified. For example, a system user ID must not be assigned to more than one person, and each user must have an individually identifiable ID.
- Each user must be identified and authenticated before performing any actions on the system.
- The authentication process is limited to five unsuccessful attempts. When this limit is reached, the user identifier should be disabled.
- Identification and authentication should both be completely processed by the system prior to displaying the failed attempt indicator. All messages associated with failed logins should be non-descriptive.
- Only a security administrator or equivalent will have the access entitlements necessary to reset a disabled user ID.
- A user identifier that has been inactive for a period of 90 days should be disabled. The intervention of a security administrator should be required to reset the disabled user ID. If an exception to this is required, the business unit manager should approve the exception condition in writing.

User Access Administration

Access Control is the process of assuring that only properly approved users are granted access to information. The goals of user Access Administration are to permit access to information and technology resources on a need-to-know basis according to job function and to ensure that users are prevented from gaining access to information and technology for which they are not authorized.

The user Access Administration policy guidance is set forth below:

- Business unit managers must authorize access to information and technology.
- Access to information and technology must be on a need-to-know, job-function basis. Users must only have the minimum access rights and privileges needed to perform a particular function or transaction.
- At least annually, a review of user access rights to information and technology must be conducted.
- At least semi-annually, a review of user IDs not used within the last six months should be conducted by the business unit to determine if these user IDs should be disabled or deleted.
- Access to technical system documentation (e.g., application documentation and user manuals) should be restricted on a need-to-know, job-function basis.
- A business unit manager should notify the security administrator immediately upon transfer, change of job responsibilities or leave of absence of a user.
- When a security administrator is notified that a user has transferred, changed job responsibilities or taken a leave of absence, the Security Administrator should immediately take steps to ensure that the user's access privileges are revoked if those privileges no longer apply.
- User accounts that have attempted to log in five times unsuccessfully should be locked until a system administrator unlocks them or until 30 minutes have passed.
- If there are 10 or more unsuccessful login attempts within a 24 hour period, the account will be permanently locked until unlocked by a system administrator.

Monitoring

Monitoring is the process of gathering information related to the interaction between users and information. This information provides a means of reconstructing events for investigative purposes and establishing individual accountability. The goals of monitoring are to provide for the logging of events and provide a mechanism to retrieve and report information on logged events.

Specific security events should be recorded, including:

- Successful session log-ins.
- Identification and authentication failures.
- Security administration activity.
- All activities performed by privileged users.
- Failed attempts to access information.

Specific information should be included in the tracking record associated with each event:

- User identifier.
- Information or system accessed.
- Date and time of access.
- Type of event.
- Result of event.
- Reason for failure (if applicable).

In addition, monitoring should include:

- The identity of the user, or processes acting on behalf of the user, should be maintained for the duration of the session. For example, change of operational mode or privileges should not result in the loss of uniqueness of a user.
- Accountability tracking information should be maintained for a minimum of three months after it is collected. Retention may be extended by legal, regulatory or investigative requirements.
- To allow proper remedial action, the operational area, business unit or information security personnel should review records reflecting security relevant events in a periodic and timely manner.

FAQ

Question: A member of our workforce attempted to log in numerous times unsuccessfully. Their account is now locked. What should they do?

Answer: User accounts that have attempted to log in five times unsuccessfully should be locked until a system administrator unlocks them or until 30 minutes have passed. If there are 10 or more unsuccessful login attempts within a 24 hour period, the account will be permanently locked until unlocked by a system administrator.

Question: What is the difference between identification and authentication?

Answer: Identification is the process of uniquely distinguishing one user from another to establish accountability. Authentication is the process of verifying the identity of a user. The goals of identification and authentication are to establish the identity of a user, verify the claimed identity, and provide accountability for the actions that the user performs.

Policy Number: 134

Date of Adoption:

Date of Review/Revision:

DATA TRANSMISSION SECURITY POLICY

Scope of Policy

This policy governs Data Transmission Security for NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to establish and implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA. The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective or providing reasonable protections for IIHI, including PHI.

Specific Data Transmission Security Procedures will be developed to protect IIHI, including ePHI. Responsibility for the development and implementation of these Data Transmission Security Procedures will reside with the CPO, CTO or other designated responsible party, who will ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.

NFP's policy is to fully document all Data Transmission Security Procedures, activities and efforts in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

Email Security and Encryption

NFP encrypts emails in transit when identified (manually or through automated algorithms) as containing PHI, PII, or other sensitive information. NFP uses third-party mechanisms to protect incoming and outgoing message queues from receiving or sending malicious content, including the vetting of all payloads and links contained therein.

Unstructured Data Storage and Transit

All file and data repositories are strictly secured by logical access control policies. Sensitive unstructured data is encrypted in flight through HTTPS, FTPS or SFTP.

FAQ

Question: What constitutes ePHI?

Answer: Electronic PHI or ePHI is defined as PHI that is transmitted by, or maintained in, electronic media. In other words, ePHI is PHI that is stored in computers and the devices that are used with computers, such as disks and drives. EPHI would also include PHI transmitted via email or in any other manner over the internet. However, ePHI does not include PHI on pieces of paper or PHI that is faxed over a dedicated phone line.

Question: I emailed some protected information to the wrong client. I've asked the client to delete the information. Do I need to do anything else?

Answer: Yes. Report the incident to NFP's CIRT, which stands ready to respond to any cybersecurity incident, even unintended disclosures that are the result of employee mistakes. Alert CIRT of incidents by emailing CIRT@nfp.com or by contacting Mark Grosvenor (mgrosvenor@nfp.com or 512.697.6650) or David Horn (dhorn@nfp.com or 512.697.6508).

Policy Number: 135
Date of Adoption:
Date of Review/Revision:

MOBILE DEVICE POLICY

Scope of Policy

This policy governs the use of mobile devices that can access, use, transmit or store IIHI and PHI in the custody of NFP. All personnel of NFP must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Policy Statement

NFP's policy is to:

- Extend all the privacy and security protections required by HIPAA to PHI accessed, used, transmitted and stored on mobile devices operated by members of our workforce.
- Include privacy and security issues related to mobile devices in our risk management process and analyses, to better understand risks inherent in the use of such devices.
- Limit the access, use, transmittal and storage of PHI exclusively to those mobile devices that can be configured and operated to deliver privacy and security comparable to the non-mobile data processing systems and devices that NFP operates.
- Limit the access, use, transmittal and storage of PHI on mobile devices to the Minimum Necessary, as that term is defined in the HIPAA Regulations.
- Train workforce members on the safe and secure usage of mobile devices that are utilized to access, use, transmit or store PHI.
- Fully document all mobile device-related activities which involve PHI in accordance with the NFP HIPAA Documentation Policy and the requirements of HIPAA.

This policy applies to all electronic computing and communications devices which may be readily carried by an individual and are capable of receiving, processing or transmitting PHI, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other mobile device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices). Mobile devices include, but are not limited to smartphones, digital music players, hand-held computers, laptop computers, tablet computers and PDAs.

This policy applies to personally-owned mobile devices as well as mobile devices owned or leased by, and provided by NFP.

Mobile devices which cannot be or have not been configured to comply with this policy are prohibited.

Procedures

Authorization

No mobile device may be used for any purpose or activity involving information subject to this policy without prior registration of the device and written authorization by the CPO, CTO or other designated responsible party. Authorization will be given only for uses of mobile devices confirmed to have been configured to be compliant with this policy.

Any access, use, transmittal or storage of PHI subject to this policy by a mobile device, and any use of a mobile device in any NFP facility or firm, including an authorized home office or remote site, must be in compliance with all NFP policies at all times.

Authorization to use a mobile device may be suspended at any time:

- If the user fails or refuses to comply with this policy
- In order to avoid, prevent or mitigate the consequences of a violation of this policy
- In connection with the investigation of a possible or proven security breach, security incident, or violation of NFP's policies
- In order to protect life, health, privacy, reputational or financial interests; to protect any assets, information, reputational or financial interests of NFP
- Upon request of a supervisor or department head in which the user works

- Upon the direction of the CPO, CTO or other designated responsible party

Authorization to use a mobile device terminates:

- Automatically upon the termination of a user's status as a member of NFP's workforce
- Upon a change in the user's role as a member of NFP's workforce, unless continued authorization is authorized in writing
- If it is determined that the user violated this or any other NFP policy, in accordance with NFP's Sanction policy.

The use of a mobile device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this policy. At any time, any mobile device may be subject to audit to ensure compliance with this and other NFP policies. Any user receiving such a request will transfer possession of the mobile device to the NFP's CPO, CTO or other designated responsible party, at once, unless a later transfer date and time is indicated in the request, and will not delete or modify any information subject to this policy which is stored on the mobile device after receiving the request.

Mobile Device & Laptop Data and Physical Security

The protection of NFP's mobile assets and the data they may contain is paramount. The following outlines NFP's Mobile Device & Laptop Data and Physical Security Policy:

While in the office:

- All laptops that have the ability must be fitted with a cable lock secured to the user's desk.
- When leaving a laptop unattended for any extended period of time, the user must physically secure the laptop with a cable lock or store it away in a locked cabinet or locked office.
- Users must always log off before leaving your workspace.
- All laptops must have full disk encryption software installed and a method of validation.
- All laptops must have a password protected screen saver that starts automatically after ten minutes of inactivity.

While out of the office:

- Laptops, tablets and smartphones (mobile devices) cannot be left in a vehicle for any extended period of time or overnight.
- In "vulnerable" situations (e.g., public areas such as airport lounges, hotels and conference centers) the mobile devices must never be left unattended; where possible the user should lock mobile devices in a hotel safe or otherwise secure the mobile devices with a cable lock.
- When boarding a plane, mobile devices should not be checked into baggage and should always be part of the user's carry-on items.
- Only secure internet connections should be used to conduct sensitive or confidential business. Examples of unsecured connections include, but are not limited to:
  - Public computers or digital copiers in hotels, airport office centers or other centers (e.g., public cafes).
  - Open, unsecured wireless internet lines available through hot spots.

When knowingly carrying sensitive information:

- Sensitive information must be stored on a secured and backed-up company file storage location.
- Sensitive information or files should not be transferred to media such as USB memory keys, CDs, DVDs, floppy disks or other portable data storage devices.
- Documents with sensitive or confidential information must be password-protected. Emailing these documents must be restricted to NFP's secure and encrypted email platform.

FAQ

Question: Does this policy apply only to smartphones?

Answer: No, this policy applies to all electronic computing and communications devices which may be readily carried by a workforce member and are capable of receiving, processing or transmitting PHI. Mobile devices include, but are not limited to smartphones, digital music players, hand-held computers, laptop computers, tablet computers and PDAs. This policy also applies to personally-owned mobile devices as well as mobile devices owned or leased by, and provided by NFP.

Compliance Department

Chief Compliance Officer

sspradley@nfp.com

Legal Department

Chief Privacy Officer

dhorn@nfp.com

Technology Department

Chief Technology Officer

mark.grosvenor@nfp.com

1250 Capital of TX Highway South, Suite 600
Austin, TX 78746