NCHIIN North Coast Health Improvement and Information Network

Policy Manual & Standards

Revised
June 2016
March 2012
May 2011
June 2010

Policy & Standards

***Derived from the Connecting for Health Common Framework**

Policy & Standards Table of Contents

Definitions

The meanings of the following terms shall be consistent throughout these policies and procedures.

Authorized User (or "User") means an individual (i.e., a person) designated to access the North Coast Health Information Network referral services on behalf of a Participant, such as an employee of a Participant, or a member of the Participant' clinical staff.

Data Provider means a Participant who provides clinical data to the referral services operated by North Coast Health Information Network.

Data Recipient means a Participant who receives clinical data from the referral services operated by North Coast Health Information Network.

Referral means the North Coast Health Information Network rules based electronic health information delivery services accessed by Authorized Users.

Individual means a person, generally a patient but possibly a caregiver for a patient, who requests access to Patient Data available from the referral services operated by North Coast Health Information Network.

Participant means an entity (e.g., a family practice, a community clinic, a laboratory, a hospital, a radiology center, etc.) that has signed a Business Associate Agreement or a Participation Agreement with North Coast Health Information Network, and that interacts with the North Coast Health Information Network Referral services as a Data Provider and/or a Data Recipient.

Business Associate Agreement means the legally binding agreement which incorporates some of the requirements set forth in the Privacy Rule (HIPAA) for covered entities.

Patient Data means electronic health, demographic and related information provided by a Data Provider to a Data Recipient via the North Coast Health Information Network referral services.

Connecting for Health's Nine Policy Principles

1. **Openness and Transparency.** Openness about developments, procedures, policies, technology and practices with respect to the treatment of personal health data is essential to protecting privacy. Individuals should be able to understand what information exists about them, how that information is used, and how they can exercise reasonable control over that information. This transparency helps promote privacy practices and instills confidence in individuals with regard to data privacy, which in turn can help increase participation in health data networks.

2. **Purpose Specification and Minimization.** Data must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

3. **Collection Limitation.** Personal health information should be obtained only by fair and lawful means and, if applicable, with the knowledge and consent of the pertinent individual. In an electronic networked environment, it is particularly important for individuals to understand how information concerning them is being collected because electronic collection methods may be confusing to average users. Similarly, individuals may not be aware of the potential abuses that can arise if they submit personal health information via an electronic method.

4. **Use Limitation.** The use and disclosure of health information should be limited to those purposes specified by the data recipient. Certain expectations such as law enforcement or security may warrant reuse of data for other purposes. However, when data is used for purposes other than those originally specified, prior de-identification of the data can help protect individual privacy while enabling important benefits to be derived from the information.

5. **Individual Participation and Control.** Every individual should retain the right to request and receive in a timely and intelligible manner information regarding who has that individual's health data and what specific data the party has, to know any reason for a denial of such request, and to challenge or amend such personal information. Because individuals have a vital stake in their own personal health information, such rights enable them to be participants in the collection and use of their data. Individual participation promotes data quality, privacy and confidence in privacy practices.

6. **Data Integrity and Quality.** Health data should be accurate, complete, relevant, and up-to-date to ensure its usefulness. The quality of health care depends on the existence of accurate health information. Moreover, individuals can be adversely affected by inaccurate health information in other arenas like insurance and employment. Thus, the integrity of health data must be maintained and individuals must be permitted to view information about them and amend such health information so that it is accurate and complete.

7. **Security Safeguards and Controls.** Security safeguards are essential to privacy protection because they help protect data loss, corruption, unauthorized use, modification and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Design and implementation of various technical security precautions such as identity management tools, data scrubbing, and hashing, auditing, authenticating and other tools can strengthen information privacy.

8. **Accountability and Oversight.** Privacy protections have little weight if privacy violators are not held accountable for compliance failures. Employee training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by holding accountable those who violate privacy requirements and identifying and correcting weaknesses in their security systems.

9. **Remedies.** The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches. Such remedies should hold violators accountable for compliance failures, reassure individuals about the organization's commitment to information privacy, and mitigate any harm that privacy violations may cause individuals.

Category 100: Compliance with Law and Policy

Version: 1.1

Privacy Principles: Openness and Transparency; Data Integrity and Quality; Accountability and Oversight; Remedies

Purpose: Policies to establish comprehensive privacy protection, compliance, enforcement procedures, and remedies following violations are crucial to maintaining health information privacy. This policy category recognizes that formal promulgation of internal North Coast Health Information Network policies and procedures ("North Coast Health Information Network Policies") which require that North Coast Health Information Network participants[1] ("Participants") comply with applicable law is an indispensable feature of essential privacy protections. When there is a conflict between North Coast Health Information Network policies and Participant policies, the policy that is most protective of individual privacy should govern decision making. This is designed to make clear that these policies provide a floor and that Participants may choose to enhance privacy protections when appropriate. This deference to more protective policies echoes the federal pre-emption requirements of HIPAA, which do not preempt more protective state privacy laws.[2]

The requirement that Participants develop internal policies will help implement the principles of sound data management practices and accountability as well as ensure that decisions affecting individuals' privacy interests are made thoughtfully, rather than on an ad hoc basis. Written documentation of such policies facilitates the training of personnel who will handle health information and enhances the accountability of Participants and the members of their workforce. Finally, the existence of internal policies for compliance by North Coast Health Information Network with applicable law creates transparency surrounding the handling and safeguarding of data by entities participating in the North Coast Health Information Network.

Scope: These policies apply to all entities participating in the North Coast Health Information Network.

Policies

101. Compliance with Laws and Regulations
102. Compliance with North Coast Health Information Network Policies
103. Compliance with Participant Policies

Policy 101: Compliance with Laws and Regulations

Version: 1.1

101. Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure constant and consistent compliance with all applicable laws and regulations.

Policy 102: Compliance with North Coast Health Information Network Privacy Policies

Version: 1.1

102. Each Participant shall, at all times, comply with all applicable North Coast Health Information Network Policies, which may be revised and updated from time to time upon reasonable written notice to Participants. Each Participant is responsible for ensuring it has a copy of and is in compliance with the most recent version of these North Coast Health Information Network Policies.

Policy 103: Participant Policies
Version: 1.1

103. Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and regulations and with the North Coast Health Information Network Policies. In the event of a conflict between North Coast Health Information Network Policies and an institution's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.

---

[1] Note that in the North Coast Health Information Network policies a "Participant" is a business entity contractually engaged with North Coast Health Information Network as a data provider and/or a data recipient. The Participant role is distinct from a "User", who is a person that is authorized by a Participant to access the North Coast Health Information Network online services, or from an "Individual", who is a person acting without affiliation with a North Coast Health Information Network Participant that requests access to patient information available from North Coast Health Information Network.

[2] 45 C.F.R. § 160.203.

Category 200: Notice of Privacy Practices
Version: 1.1

Principles: Openness and Transparency; Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control.

Purpose: These policies incorporate HIPAA requirements obligating entities to provide a notice of the privacy practices to individuals upon request.[1]

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network.

Policies

201. Content of the Notice of Privacy Practices
202. Provision of the Privacy Notice to Individuals
203. Individual Acknowledgement of the Privacy Notice

Policy 201: Content of the Notice of Privacy Practices
Version: 1.1

201. Each Participant shall develop and maintain a notice of privacy practices (the "Notice") that complies with applicable law and with these policies. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule[2] and comply with all applicable laws and regulations.

Policy 202: Provision of the Privacy Notice to Individuals
Version: 1.1

202. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and such policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

    For Participants that are health care providers, the Notice shall be:

    (i) Available to the public upon request
    (ii) Provided to a patient at the date of first service delivery
    (iii) Available at the institution

(iv) Posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.[3]

Policy 203: Individual Acknowledgement of the Privacy Notice

Version: 1.1

203. Each Participant that is a health care provider shall make a good faith effort to obtain each individual's written acknowledgment of receipt of the Notice or to document their efforts and/or failure to do so. The acknowledgment of the Notice shall comply with all applicable laws and regulations.[4] Each Participant shall have its own policies and procedures governing the process of obtaining an acknowledgment, and such policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

---

[1] 45 C.F.R. § 164.520.
[2] 45 C.F.R. § 164.520(b).
[3] 45 C.F.R. § 164.520(c)(2), (3).
[4] 45 C.F.R. § 164.520(c)(2)(ii).

Category 300: Uses and disclosures of Health Information

Version: 1.1

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight.

Purpose: These policies integrate the general premise of HIPAA that health information may be used only for permissible purposes and its more specific requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.[1] In general, requests for disclosure of and/or use of health information for treatment, payment, and the health care operations of a covered entity, as each is defined by HIPAA, will be permitted.[2] Furthermore, subject to certain limitations, and under certain circumstances, requesting disclosure of and using health information for law enforcement,[3] disaster relief,[4] research,[5] and public health[6] purposes also may be permissible. Under no circumstances may health information be accessed or used for discriminatory purposes.

Requiring consideration of the purpose of a use and minimization of the use of information reduces the likelihood of inadvertent or intentional misuses of information. By ensuring that Participants have legally required documentation prior to the use or disclosure of information, these policies help enhance the fair and legal collection and use of data, the oversight of data use and accountability for privacy violations.[7] In addition, the integration of HIPAA's accounting of disclosures and individual access to information requirements allows individuals to understand how health information about them is shared and to exercise certain rights regarding information about them.[8]

These policies also require security measures essential to identify and remedy loss, unauthorized access, destruction, use, modification, or disclosure of personal health information. Entities should implement policies to prevent security violations, assess security risks, and examine data storage and access technology.[9] To prevent unauthorized access of information and maintain data integrity and quality, the authentication provision of this policy requires that both the identity and authority of an entity requesting health information be verified and authenticated, integrating requirements from the HIPAA Privacy Rule and Security Rule.[10]

The combination of these policies' use and security provisions helps guarantee that health information is used and accessed only as authorized and that Participants have proper measures in place to identify and address privacy violations.

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network.

Policies

301. Definition of Disclosure
302. Disclosure Compliance with Laws and Regulations
303. Permissible Purposes Required for Use or Disclosure
304. Disclosure Compliance with North Coast Health Information Network Policies
305. Disclosure Compliance with Participant Policies
306. Accounting of Disclosures
307. Disclosure Audit Logs
308. Disclosure Authentication Requirements
309. Disclosure Access Process
310. Occurrence of a Health Information Breach

Policy 301: Definition of Disclosure

Version: 1.1

301. Disclosure of health information in the North Coast Health Information Network policies is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."[11]

Policy 302: Disclosure Compliance with Laws and Regulations

Version: 1.1

302. All disclosures of health information through the North Coast Health Information Network and the use of information obtained from the Network shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing institution.[12]

Policy 303: Permissible Purpose Required for Use or Disclosure

Version: 1.1

303. A Participant may request health information through North Coast Health Information Network only for purposes permitted by applicable law. Each Participant shall provide or request health information through the Network only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations, [13] and by these North Coast Health Information Network Policies. Information may not be requested for marketing or marketing related purposes. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request information through the Network.

Policy 304: Disclosure Compliance with North Coast Health Information Network Policies

Version: 1.1

304. Uses and disclosures of shall comply with all North Coast Health Information Network Policies, including, but not limited to, the North Coast Health Information Network Minimum Necessary Use of Health Information (600s).[14]

Policy 305: Disclosure Compliance with Participant Policies
Version: 1.1

305. Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and the documentation that shall be obtained, if any, prior to making such disclosures.

Policy 306: Accounting of Disclosures
Version: 1.1

306. Each Participant disclosing health information through the North Coast Health Information Network shall document the purposes for which such disclosures are made, as provided by the requesting institution, and any other information that may be necessary for compliance with the disclosure requirements of the HIPAA Privacy Rule.[15] Each Participant is responsible for ensuring its compliance with such requirements and may choose to provide Individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the accounting of disclosures requirement of the HIPAA Privacy Rule.

Policy 307: Disclosure Audit Logs
Version: 1.1

307. North Coast Health Information Network shall maintain an audit log documenting which Participants have posted information and which Participants have received information.[16] North Coast Health Information Network shall implement a system allowing patients to request and receive a listing of who has posted and which entities have received information about them. Individual patient requests for audit information are exercised through the Participant.

Policy 308: Disclosure Authentication Requirements
Version: 1.1

308. Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating Users within their institutions who have access to information through the North Coast Health Information Network .[17] [18]

Policy 309: Disclosure Access Process
Version: 1.1

309. North Coast Health Information Network will establish a formal process through which information in the Network can be requested by a patient or on a patient's behalf.[19]

Policy 310: Occurrence of a Health Information Breach
Version: 1.1

310. As set forth under HIPAA and ARRA[20], notification to individuals is required if their health information has been breached. Breach is defined as the unauthorized acquisition, access, use or disclosure of protected health information. However, it is not a breach:
    - Where an unauthorized person who receives the health information cannot reasonably have been able to retain it;
    - If an unintentional acquisition, access or use occurs within the scope of employment or a professional relationship and the information does not go any further (i.e., it is not further

acquired, accessed, used or disclosed); or

- It is an inadvertent disclosure that occurs within a Participant facility, and the information does not go any further.

Only breaches of "unsecured" health information trigger the notification requirement.

---

[1] 45 C.F.R. § 164.502(b).

[2] 45 C.F.R. § 164.502(1)(ii), 506. Under HIPAA, treatment is defined as "the provision, coordination, or management of health care and related services by one or more health care providers ... " 45 C.F.R. § 164.501. Payment refers to "activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care." Id. Such activities include eligibility and coverage determinations; risk adjustments; billing, claims management and collection activities; medical necessity review; and utilization review. Health care operations includes activities related to covered functions for (i) conducting quality assessment and improvement; (ii) evaluating competence, qualifications and performance of health care professionals, evaluating health plan performance, training and credentialing activities; (iii) underwriting, "premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits"; (iv) "conducting or arranging for medical review, legal services, and auditing functions;" (v) business planning and development; and (vi) business management and administrative activities. Id.

[3] 45 C.F.R. § 164.512(f).

[4] 45 C.F.R. § 164.510(b)(4).

[5] 45 C.F.R. § 164.512(i).

[6] 45 C.F.R. § 164.512(b).

[7] 45 C.F.R. § 164.530(j).

[8] 45 C.F.R. § 164.528; 164.524.

[9] 45 C.F.R. § 164.316, 164.308(a)(1)(i).

[10] 45 C.F.R. § 164.514(h), 164.312(d).

[11] 45 C.F.R. § 160.103.

[12] 45 C.F.R. § 164.530(j).

[13] 45 C.F.R. § 164.502(a), (b).

[14] 45 C.F.R. § 164.502(b).

[15] 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law.

[16] 45 C.F.R. § 164.316, 164.308(a)(1)(i).

[17] 45 C.F.R. § 164.514(h), 164.312(d).

[18] The Markle Foundation, **Authentication of System Users**, Connecting for Health Common Framework: sources for Implementing Private and Secure Health Information Exchange (2006).

[19] 45 C.F.R. § 164.524.

[20] ARRA Section 13402

Category 400: Information Subject to Special Protection

Version: 1.1

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control; Data Integrity and Quality; Security Safeguards and Controls.

Purpose: These policies facilitate individualized privacy protections by requiring Participants to heed any special protections of specific information types as set forth under applicable laws or regulations. In complying with these special protections, the collection, use and disclosure of health information by Participants is limited to legitimate purposes. Moreover, in guaranteeing deference to the law or policy

most protective of privacy, the provisions below echo the federal preemption requirements of HIPAA which defer to state laws that are more protective than the privacy provisions of HIPAA.[1]

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network, and that may provide or make available health information through the Network.

Policies

401. Information Subject to Special Protection

Policy 401: Information Subject to Special Protection

Version: 1.1

401. Some health information may be subject to special protection (e.g., substance abuse, mental health, HIV, STI, etc.). Each Participant shall determine and identify what information is subject to special protection under applicable federal, state, and/or local law prior to disclosing any information through the Network. Each Participant is responsible for complying with such laws and regulations.

[1] The Markle Foundation, Patients' Access to Their Own Health Information, Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange (2006).

Category 500: Minimum Necessary

Version: 1.1

Principles: Collection Limitation; Use Limitation; Data Integrity and Quality; Security Safeguards and Controls.

Purpose: These policies incorporate the HIPAA requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.[1] The policies exempt treatment disclosures from this minimum necessary requirement to balance the protection of privacy with the provision of quality health care. In assessing the smallest amount of information that is necessary to accomplish a particular purpose, Participants are less likely to collect, use or disclose information for an unauthorized purpose. Minimal collection, access, use and disclosure increases public confidence in the privacy practices of Participants, enhances information privacy, and diminishes the potential for data corruption and security violations.

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network, and that may provide, make available, or request health information through the Network.

Policies

501. Minimum Necessary Use of Health Information
502. Minimum Necessary Disclosure of Health Information
503. Minimum Necessary Health Information Requests

Category 501: Minimum Necessary Use of Health Information

Version: 1.1

501. Each Participant shall use only the minimum amount of health information obtained through the Network as is necessary for the specific purpose of such use. Each Participant shall share health information obtained through the Network, and shall allow access to such information by only those workforce members, agents, and contractors who need the specific information in connection with their job function or duties.

Policy 502: Minimum Necessary Disclosure of Health Information
Version: 1.1

502. Each Participant shall disclose through the Network only the minimum amount of health information as is necessary for the specific purpose of the disclosure. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

Policy 503: Minimum Necessary Health Information Requests
Version: 1.1

503. Each Participant shall request only the minimum amount of health information through the North Coast Health Information Network as is necessary for the intended purpose of the request. This Minimum Necessary Policy does not apply to requests by qualified health care providers for treatment purposes.

[1] 45 C.F.R. § 164.502(b).

Policy 600: Workforce, Agents, and Contractors
Version: 1.1

Principles: Use Limitation; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight; Remedies.

Purpose: These policies incorporate the HIPAA administrative requirements for workforce training, sanctions for privacy violations, and the reporting of complaints.[1] Because a Participant's workforce is responsible for implementation of privacy practices, proper training is vital to ensure the legitimate use of health information and the prompt identification, reporting, and correction of any security vulnerability or privacy spill. Individual accountability in the form of sanctions for those persons responsible for privacy violations is fundamental to encouraging compliance with privacy practices. Without such incentive for compliance, privacy violations and security risks may go unchecked and lead to larger privacy problems. Similarly, providing for the reporting of non-compliance enables Participants to discover and correct privacy violations and identify and sanction privacy violators. These policies help guarantee the legitimate use of health data, the proper implementation of Participants' privacy practices, and the prompt identification of and undertaking of remedial action for privacy violations.

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network.

Policies
601. Participant Access to North Coast Health Information Network Services
602. Participant Training for Use of North Coast Health Information Network Services
603. Participant Discipline for Non-Compliance
604. Participant Reporting of Non-Compliance
605. Suspended Access for Persistent Non-Compliance

Policy 601: Participant Access to North Coast Health Information Network Services
Version: 1.1

601. Each Participant shall allow access to the Network only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the Network. No workforce member,

agent, or contractor shall be provided with access to the North Coast Health Information Network without first having been trained on these Policies.

Policy 602: Participant Training for Use of North Coast Health Information Network Services
Version: 1.1

602. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the Network to ensure compliance with these Policies.[2] The training shall include a detailed review of applicable North Coast Health Information Network's Privacy Policies and each trained workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these Policies.

Policy 603: Participant Discipline for Non-Compliance
Version: 1.1

603. Each Participant shall implement clearly defined procedures to discipline and hold workforce members, agents, and contractors accountable to ensure that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies.[3] Such discipline measures shall include, but not be limited to, verbal and written warnings, and shall provide for retraining where appropriate.

Policy 604: Participant Reporting of Non-Compliance
Version: 1.1

604. Each Participant shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any non-compliance with these Policies to the Participant[4]. Each Participant also shall establish a process for individuals whose health information is included in the RLS to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

Policy 605: Suspended Access for Persistent Non-Compliance
Version: 1.1

605. Each Participant shall be subject to denial of access to the Network if repeated efforts to train and discipline all workforce members, agents and contractors of that Participant result in persistent non-compliance with these policies.

---

[1] 45 C.F.R. § 164.530.
[2] 45 C.F.R. § 164.530(b).
[3] 45 C.F.R. § 164.530(e).
[4] 45 C.F.R. § 164.530(a), (d).

Category 700: Amendment of Data
Version: 1.1

Principles: Openness and Transparency; Individual Participation and Control; Data Integrity and Quality; Accountability and Oversight.

Purpose: These policies integrate the right granted to Individuals by the HIPAA Privacy Rule to amend health information about them under certain circumstances[1]. Accurate health information not only is indispensable to the delivery of health care, but is important to individuals' applications for insurance and employment and in a variety of other arenas. Allowing individuals to verify the accuracy and

completeness of information concerning them contributes to the transparency of Participants' operations and fosters confidence in Participants' privacy practices and commitment to data accuracy. These policies will enable Participants to more readily rely upon the integrity and quality of their health care data and more easily monitor, account for, and remedy systemic data inaccuracies, corruption, and other data deficiencies or privacy lapses.

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network.

Policies

701. Amendment of Individual Data

Policy 701: Amendment of Individual Data

Version: 1.1

701. Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.[2] If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant shall make reasonable efforts to inform other Participants that accessed or received such information through the Network, within a reasonable time, if the recipient institution may have relied or could foreseeably rely on the information to the detriment of the individual.

[1] 45 C.F.R. § 164.526.

[2] 45 C.F.R. § 164.526.

Category 800: Requests for Restrictions

Version: 1.1

Principles: Use Limitation; Individual Participation and Control; Accountability and Oversight.

Purpose: These policies require Participants who agree to individual requests for restrictions in accordance with the HIPAA Privacy Rule to comply with such requests with regard to the release of information from the Network.[1] Such compliance ensures permissible use of health information and accountability on the part of Participants who agree to individually requested use restrictions. Without the ability to request restrictions and without assurance that Participants will honor these agreed-upon restrictions, Individuals may remain silent about important information that could affect their health. By creating confidence in Participants and their privacy protections and encouraging individual participation, these policies foster dialog between individuals and Participants, thereby reinforcing traditional standards of confidentiality between a patient and their health care provider. Effective communication between a provider and a patient improves the overall delivery of health care.

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network.

Policies

801. Individual Requests for Restrictions

Policy 801: Individual Requests for Restrictions

Version: 1.1

801. If a Participant agrees to an Individual's request for restrictions,[2] as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing

information through the Network. If an agreed-upon restriction will or could affect the requesting institution's uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting (or referred to) institution of the fact that certain information has been restricted, without disclosing the content of any such restriction.

[1] 45 C.F.R. § 164.522.

[2] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA

Category 900: Mitigation

Version: 1.1

Principles: Openness and Transparency; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight; Remedies.

Purpose: These policies incorporate the HIPAA requirement that entities have procedures and take steps to mitigate harm resulting from an impermissible use or disclosure of health information[1]. Without the duty to mitigate harm from privacy violations, Participants may not promptly address data security weaknesses or breaches which could lead to greater privacy lapses in the future, diminish the confidence that Individuals have in Participants' privacy practices, and compromise the accuracy, integrity, and quality of Participants' data. Remedial action and mitigation are essential both to reassure individuals that Participants are vigilant in addressing privacy violations and ameliorating any harm from such violations and to help Participants ensure that their data oversight practices and security measures are functioning and effective.

Scope: These policies apply to all entities that are participating in the North Coast Health Information Network.

Policies

901. Appropriate Remedial Action
902. Breach Notification

Policy 901: Appropriate Remedial Action

Version: 1.1

901. Each Participant shall recognize, mitigate and take appropriate remedial action, to the extent practicable, in response to any harmful effect that is known to the institution of a use or disclosure of health information through the North Coast Health Information Network in violation of applicable laws and/or regulations and/or these North Coast Health Information Network Privacy Policies by the institution, or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Participant notification to the Individual of the disclosure of information about them or Participant request to the party who received such information to return and/or destroy the impermissibly disclosed information.

Policy 902: Public Breach Notification

Version: 1.1

902. Breaches of unsecured health information trigger the notification requirement. Notice must be afforded no later than 60 days after the discovery of the breach. A breach is considered to be

"discovered" when at least one employee of the Participant (other than the person responsible for the breach) knows, or reasonably should know, about the breach. Notice is required to be provided to media outlets if the information of more than 500 individuals is involved. Notice of all breaches must also be provided to the Secretary of the U.S. Department of Health and Human Services. This notice must be immediate if the breach involves the information of more than 500 individuals. These breach provisions do not expressly preempt any applicable State breach notification laws or regulations.

[1] 45 C.F.R. § 164.530(f).